Centre de la sécurité des télécommunications
Communications Security Establishment

Conseils en matière de sécurité des TI

MANUEL SUR LA COMMANDE DE CLÉS CRYPTOGRAPHIQUES

MAI 2006

ITSG-13

Canada

Page intentionnellement laissée en blanc

Avant-propos

Le *Manuel sur la commande de clés cryptographiques* (ITSG-13) est un document non classifié publié avec l'autorisation du chef du Centre de la sécurité des télécommunications (CST). Il incombe au CST, à titre d'organisme principal pour les questions cryptographiques au gouvernement du Canada (GC), d'approuver la production et l'utilisation de l'équipement cryptographique, de fournir du matériel de chiffrement cryptographique et de la documentation connexe autant aux ministères du gouvernement fédéral qui gèrent de l'information classifiée et désignée qu'à l'industrie, dans le cadre d'un contrat avec le gouvernement, d'un parrainage ou d'un partenariat fédéral.

La présente publication entre en vigueur dès sa réception et remplace les documents *Plan de gestion des clés STU III* (CID/01/13) en date d'octobre 1994 et *Directive sur le contrôle des clés STU III – Applications touchant aux renseignements cloisonnés de nature délicate* (NITSM 4/90), en date de novembre 1990.

Toutes les propositions de modifications doivent être envoyées au chef du Centre d'assistance et de gestion du matériel cryptographique (CAGMC) du CST, et ce, par les voies responsables de la sécurité des télécommunications au sein de votre ministère.

Toutes les demandes relatives à des exemplaires supplémentaires, à des modifications à apporter dans la distribution de la présente publication ou à des exemplaires d'autres publications mentionnées en bibliographie devraient être adressées au chef du CAGMC du CST, par courriel à cmac@cse-cst.gc.ca ou par téléphone au (613) 991-8826.

Directrice, Gestion de la mission de la Sécurité des TI

Sue Greaves

© 2006 Gouvernement du Canada, Centre de la sécurité des télécommunications (CST)

C.P. 9703, Terminus, Ottawa (Ontario), Canada, K1G 3Z4

Cette publication peut être reproduite dans son intégralité et sans frais à des fins éducatives et individuelles. Toutefois, pour utiliser le contenu du document sous forme modifiée ou d'extrait, ou pour tout usage commercial, il faut obtenir au préalable la permission écrite du CST.

Page intentionnellement laissée en blanc

Registre des modificatifs

Modificatif n^{o}	Date	Inscrit par

Page intentionnellement laissée en blanc

Table des matières

1 Introduction 1
1.1 Objet 1
1.2 Portée 1
1.3 Champ d'application 1
1.4 Restrictions 1
1.5 Exceptions 1
1.6 Structure du document 2

2 Concepts liés aux clés et à la gestion des clés 3
2.1 Contexte 3
2.2 Aperçu de l'EKMS GC 4
2.2.1 Généralités 4
2.2.2 Installation centrale canadienne (ICC) 4
2.3 Clés cryptographiques de l'EKMS GC 6
2.3.1 Clés traditionnelle et moderne 6
2.3.2 Identification des clés 7
2.3.3 Objet des clés cryptographiques 10
2.3.4 Sources des clés cryptographiques 11
2.3.5 Applications des clés cryptographiques 11
2.3.6 Caractéristiques des clés cryptographiques 12
2.4 Processus de gestion des clés 12
2.4.1 Aperçu 12
2.4.2 Établissement des besoins en communications sécurisées 13
2.4.3 Établissement d'un compte COMSEC 13
2.4.4 Inscription des privilèges de commande de clés 13
2.4.5 Commande de clés 14
2.4.6 Contrôle de l'utilisation des clés 15
2.4.7 Remplacement des clés 15
2.4.8 Comptabilité COMSEC 15

3 Rôles et responsabilités en matière de commande de clés 17
3.1 Aperçu 17
3.2 Agent de sécurité du ministère (ASM)/Autorité COMSEC du ministère (ACM) 17
3.3 Autorité de contrôle 18
3.4 Privilèges de commande de clés traditionnelles 18
3.4.1 Gestionnaire des privilèges de commande (OPM) 18
3.4.2 Demandeur d'attribution de titre abrégé (STAR) 19
3.4.3 ID autorisé (Auth ID) 19
3.5 Privilèges de commande de clés modernes 19
3.5.1 Autorité de gestion des clés (AGC) 19
3.5.2 Représentant des utilisateurs (RU) 20
3.6 Privilèges de commande de clés américaines 20
3.6.1 Généralités 20
3.6.2 *U.S. Command Authority* (Autorité de commande américaine) 20
3.6.3 Représentant des utilisateurs américains 20

4 Inscription et gestion des privilèges 21
4.1 Généralités 21
4.1.1 Inscription 21
4.1.2 Gestion des privilèges 22
4.1.3 Commande de clés 23
4.2 Formulaires et avis 24
4.3 Certificat de nomination 25
4.3.1 Généralités 25
4.3.2 Nouvelle nomination 25
4.3.3 Changement de personnel 26
4.4 Formulaire Demande d'établissement de privilèges (PER) pour clés STU III 26
4.4.1 Généralités 26
4.4.2 Type de demande 26
4.4.3 Code DAO 26
4.4.4 Description DAO 27
4.4.5 Indicateur d'utilisation EKMS 28
4.4.6 Demande de privilèges de commande pour d'autres comptes EKMS 28
4.4.7 Type de clé autorisée 28
4.4.8 Classification maximale de la clé 29
4.4.9 Codes de Classe 6 29
4.5 Formulaire de demande d'établissement de privilèges (PER) pour clés SDNS 30
4.5.1 Généralités 30
4.5.2 Type de demande 30
4.5.3 Demande de privilèges de commande pour d'autres ID EKMS 30
4.5.4 Code de partition 30
4.5.5 Type de clé autorisée 31
4.5.6 But de la clé 32
4.6 Formulaire Demande d'établissement de privilèges (PER) pour clés MSK 32
4.6.1 Demande de privilèges de commande pour d'autres ID EKMS 33
4.6.2 Type de demande 33
4.7 Formulaire Demande d'établissement de privilèges (PER) pour clés traditionnelles 33
4.8 Avis de confirmation/rejet de PER (CRN de PER) 33
4.9 Avis de privilège de commande (OPN) 33
5 Commande de clés 35
5.1 Processus de commande de clés 35
5.1.1 Aperçu 35
5.1.2 Interaction avec les utilisateurs afin de déterminer leurs besoins en matière de clés 35
5.1.3 Validation de l'information de sécurité 35
5.1.4 Préparation de la commande de clés 35
5.1.5 Présentation d'une demande de clé 36
5.1.6 Classification/protection d'une demande de clé 36

5.1.7 Validation d'une demande de clé 36
5.1.8 Surveillance de l'état de la demande de clé 37
5.1.9 Avis aux gardiens COMSEC 37
5.2 Formulaire Demande de clé STU III 37
5.2.1 Généralités 37
5.2.2 Numéro de transaction EKMS 37
5.2.3 Type de clé 37
5.2.4 Commande de clés STU III EKMS 38
5.2.5 Mécanisme de livraison 38
5.2.6 Classification de la clé 39
5.2.7 Code de Classe 6 39
5.2.8 Code DAO 40
5.2.9 Données d'identification additionnelles 40
5.2.10 Observations 40
5.3 Formulaire Demande de clé SDNS 40
5.3.1 Généralités 40
5.3.2 Numéro de transaction 40
5.3.3 Code de partition 41
5.3.4 Type d'équipement 41
5.3.5 Type de clé 41
5.3.6 Contrôle d'accès 42
5.3.7 ID ASCII 42
5.3.8 Mécanisme de livraison 42
5.4 Formulaire Demande de clé MSK 43
5.4.1 Généralités 43
5.4.2 ID de la transaction 43
5.4.3 Type de clé 43
5.4.4 Indicateur d'utilisation EKMS 43
5.4.5 ID additionnels 44
5.5 Formulaire Demande de clés traditionnelles 44
5.5.1 Généralités 44
5.5.2 Numéro de la transaction 44
5.5.3 Types de commande 44
5.5.4 Titre abrégé 45
5.5.5 Contrôle de la distribution 45
5.5.6 Titre abrégé compatible 45
5.5.7 ID autorisés 45
5.5.8 Mécanisme de livraison 46
5.5.9 Mise en garde CRYPTO 46
5.5.10 Restrictions de traitement 46
5.5.11 Diffusion 46
5.5.12 Utilisation de la clé 46
5.5.13 But de la clé 47
5.5.14 Taille du réseau cryptographique 47
5.5.15 Cryptopériode 47
5.5.16 Segment par édition 47

5.5.17 Fréquence de remplacement 47
5.5.18 Date d'entrée en vigueur 47
5.5.19 Date de mise en place 47
5.5.20 Commande permanente 48
5.5.21 Information sur l'édition 48
5.5.22 Profil de distribution 48
5.5.23 Code de comptabilité (CC) et règles de lancement de rapport de transfert (TRI) 48
5.6 Avis de confirmation/rejet de la commande (CRN de commande) 49

Annexe A – Points de contact au CST 65

Annexe B – Directive sur le contrôle des clés STU III pour les applications SCI 67

Annexe C – Certificat de nomination 69

Annexe D – Demande d'établissement de privilèges (PER) pour clés STU III 71

Annexe E – Demande d'établissement de privilèges (PER) pour clés SDNS 73

Annexe F – Demande d'établissement de privilèges (PER) pour clés de signature de message (MSK) 75

Annexe G – Demande d'établissement de privilèges (PER) pour clés traditionnelles 77

Annexe H – Demande d'établissement de privilèges - avis de confirmation/rejet (PER CRN) 79

Annexe I – Avis de demande de privilèges (OPN) 81

Annexe J – Demande de clé STU III 83

Annexe K – Demande de clés - SDNS 85

Annexe L – Demande de clés de signature de message (MSK) 87

Annexe M – Demande de clés traditionnelles 89

Liste des figures

Figure 1 – EKMS GC 4
Figure 2 – Fonctions de gestion des clés 13
Figure 3 – Hiérarchie des privilèges de commande 17
Figure 4 – Inscription des privilèges de commande de clés modernes 21
Figure 5 – Inscription des AGC/OPM 22
Figure 6 – Inscription des RU/STAR 22
Figure 7 – Gestion des privilèges – PER rejetée par le CAGMC 23
Figure 8 – Processus de commande de clés 24

Page intentionnellement laissée en blanc

Liste des tables

Tableau 1 – Exemples de titres abrégés de clés STU III 7
Tableau 2 – Exemples de titres abrégés de clés SDNS 8
Tableau 3 – Exemples de titres abrégés de clés MSK 8
Tableau 4 – Exemples de titres abrégés de clés traditionnelles 9
Tableau 5 – Exemples d'édition de matériel cryptographique 9
Tableau 6 – Formulaires de demande d'inscription et de gestion de privilèges 24
Tableau 7 – Formulaires et avis de commande de clés 36

Page intentionnellement laissée en blanc

Liste des abréviations et des acronymes

ACM	Autorité COMSEC du ministère
AGC	Autorité de gestion des clés
AND	Autorité nationale de distribution
ASCII	American Standard Code for Information Exchange
ASM	Agent de sécurité du ministère
Auth ID	ID autorisé
BET	Transaction chiffrée en vrac
CAGMC	Centre d'assistance et de gestion du matériel cryptographique
CC	Code de comptabilité
CCD	Doctrine canadienne en matière de cryptographie
CCEB	Combined Communications Electronic Board
CCI	Article cryptographique contrôlé
CKMU	Unité canadienne de gestion des clés
COMSEC	Sécurité des télécommunications
CRN	Avis de confirmation/rejet
CRYPTO	Cryptographique
CST	Centre de la sécurité des télécommunications
DAO	Ministère ou organisme d'appartenance
DTD	Dispositif de transfert des données
EKMS GC	Système de gestion électronique des clés du GC
EKR	Remplacement électronique des clés
FFK	Clé FIREFLY
GC	Gouvernement du Canada
ICC	Installation centrale canadienne
ICP GC	Infrastructure à clé publique du GC
IFC	Infrastructure fondée sur l'emploi de certificats
IKMS	Système de gestion de clés IRIS
IPC ICC	Installation de production de clés de l'Installation centrale canadienne
KEK	Clé de chiffrement de clés
KMID	Numéro d'identification de matériel de chiffrement
KP	Processeur de clés
KPK	Clé de production de clés
KSD	Dispositif de stockage de clés

LAN	Réseau local
LMD	Dispositif de gestion locale
MDN	Ministère de la Défense nationale
MSK	Clé de signature de message
NCOR	Bureau national des dossiers
NFK	Clé FIREFLY à réseau
OPM	Gestionnaire des privilèges de commande
OPN	Avis de privilège de commande
OTAN	Organisation du Traité de l'Atlantique Nord
PCM	Gestionnaire des certificats de privilèges
PER	Demande d'établissement de privilèges
PGS	Politique du gouvernement sur la sécurité
QKEK	Clé de chiffrement de clés quadrant
RA	Autorité d'inscription
RCG	Réseau cryptophonique gouvernemental
SCGC	Système canadien de gestion des clés (maintenant le RCG)
SCCR	Système canadien de chiffrement réseau
SDNS	Secure Data Network System
SGC du RCG	Système de gestion des clés du Réseau cryptophonique gouvernemental
SNCMC	Système national de contrôle du matériel COMSEC
STAR	Demandeur d'attribution de titre abrégé
STE	Appareil terminal sécurisé
STU III	Poste cryptophonique de troisième génération
TEK	Clé de chiffrement du trafic
TPI	Intégrité par deux personnes
TrKEK	Clé de chiffrement de clé de transfert
WAN	Réseau étendu

1 Introduction

1.1 Objet

Le présent document énonce les normes de sécurité minimales en matière de commande de clés cryptographiques auprès de l'Installation centrale canadienne (ICC) du CST pour l'équipement cryptographique de type 1 et de type 2 pris en charge par le système EKMS du gouvernement du Canada (EKMS GC).

1.2 Portée

Ce manuel présente un aperçu général des concepts en matière de clés cryptographiques. Il décrit la division des responsabilités entre les diverses entités prenant part à la gestion des clés, donne la marche à suivre pour demander des privilèges de commande de clés et explique les étapes requises pour commander manuellement ou électroniquement des clés cryptographiques canadiennes et américaines auprès de l'ICC.

En cas de conflit avec les autres directives publiées, en l'occurrence le *Manuel d'exploitation du STU III* (MG-7), le présent document a préséance.

NOTE : Pour commander une clé d'un compte COMSEC pourvu d'un dispositif de gestion locale/processeur de clés (LMD/KP), veuillez consulter le document *Manuel de l'opérateur du LMD/KP* (EKMS 704).

1.3 Champ d'application

Le présent manuel s'applique à tous les ministères du GC figurant aux Annexes I, I.1 et II de la *Loi sur la gestion des finances publiques (LGFP)*, y compris les Forces canadiennes (FC), la Gendarmerie royale du Canada (GRC) et le Service canadien du renseignement de sécurité (SCRS), désignés ci-après sous le nom de ministères. Comme l'indique la Politique de sécurité du gouvernement (PSG), « les ministères doivent utiliser des méthodes de chiffrement ou d'autres mesures entérinées ou approuvées par le CST pour protéger les communications électroniques véhiculant des renseignements classifiés et de nature extrêmement délicate. » Bien que les ministères doivent utiliser une solution de type 1 pour l'information classifiée, ils peuvent utiliser, pour l'information désignée PROTÉGÉ A ou PROTÉGÉ B, certaines solutions commerciales, qui devraient néanmoins être homologuées par le CST.

1.4 Restrictions

Le présent manuel traite de l'établissement des privilèges de commande de clés cryptographiques auprès de l'ICC et de la commande de clés proprement dite par des comptes non automatisés. Pour les comptes automatisés (c.-à-d. qui utilisent le LCMS), on devrait employer ce manuel de concert avec le *Manuel de l'opérateur du LMD/KP* (EKMS 704).

1.5 Exceptions

Toutes demandes d'exceptions à l'application des procédures énoncées dans le présent manuel devraient être adressées au chef du CAGMC du CST.

1.6 Structure du document

Le présent manuel décrit les types de clés disponibles auprès du CAGMC au CST et décrit en détail les processus établis pour la commande de chacun d'eux. Les annexes contiennent les formulaires à remplir pour commander les clés ainsi que les instructions pour chaque formulaire.

2 Concepts liés aux clés et à la gestion des clés

2.1 Contexte

Depuis plus de 50 ans, il incombe au CST, à titre d'autorité nationale pour le matériel COMSEC au Canada, de générer et de produire des clés cryptographiques à l'appui des besoins nationaux et de l'OTAN. Jusqu'à la dernière décennie, les clés étaient principalement produites et distribuées sous forme physique non chiffrée. Ces clés physiques non chiffrées circulent par de nombreuses mains avant d'être insérées dans l'équipement de destination, ce qui ouvre la possibilité à leur compromission par toute personne y ayant accès. Afin d'accroître la sécurité, on effectue fréquemment une mise à jour des clés, ce qui assure que les messages chiffrés ultérieurement ne seront pas compromis par des clés antérieurement divulguées.

En 1989, le Système canadien de gestion des clés (SCGC) a été instauré pour la commande, la génération, la production et la gestion des clés cryptographiques à l'appui du Réseau cryptophonique gouvernemental (RCG). Ce réseau utilise le poste cryptophonique de troisième génération STU III (de l'anglais *Secure Telephone Unit*). Le STU III est un appareil téléphonique à double utilisation : il joue à la fois le rôle d'un téléphone ordinaire et celui d'un dispositif de communication sûre pouvant chiffrer, transmettre et déchiffrer la voix et les données. L'introduction de ce système de gestion électronique des clés a réduit ou éliminé l'accès aux clés en clair, car il chiffre ces clés et les distribue sous forme électronique depuis le point de génération jusqu'au point d'utilisation, dans la mesure du possible.

Après la mise en œuvre du SCGC, un autre système de gestion électronique des clés, le Système de gestion de clés IRIS (IKMS), a été mis au point pour répondre à une exigence particulière des FC. Ce système est devenu opérationnel en 2000. L'IKMS permet la génération décentralisée des clés et la distribution de clés chiffrées à l'aide d'une unité canadienne de gestion des clés (CKMU). Pour plus d'information sur l'IKMS et la CKMU, veuillez consulter la *Doctrine canadienne en matière de cryptographie visant l'unité canadienne de gestion des clés (CKMU)* (CCD-05).

En 2001, la gestion des clés au GC a été améliorée afin de prendre en charge l'équipement SDNS (*Secure Data Network System*, p. ex., TACLANE ou le processeur de clés KP) et de réduire davantage l'accès aux clés en clair en chiffrant ces clés et en les distribuant sous forme électronique ou physique. Ce nouveau système de gestion des clés s'appelle EKMS GC et comprend le SCGC, maintenant connu sous le nom de Système de gestion des clés du Réseau cryptophonique gouvernemental (SGC du RCG). L'EKMS GC est l'un des trois systèmes nationaux de gestion des clés exploités par l'Installation centrale canadienne (ICC) du CST. Les deux autres systèmes sont l'Infrastructure à clé publique du GC (ICP GC) et l'Infrastructure fondée sur l'emploi de certificats FORTEZZA GC (IFC FORTEZZA GC). Aux fins de la présente publication, toutes les références à l'ICC portent uniquement sur le volet EKMS GC de l'ICC. Les responsabilités de l'ICC associées à l'ICP GC et à l'IFC FORTEZZA GC sont décrites dans des documents séparés.

2.2 Aperçu de l'EKMS GC

2.2.1 Généralités

L'EKMS GC permet de commander, générer, produire, distribuer et comptabiliser les clés nationales, alliées ainsi que de l'OTAN, et ce, sous forme physique et électronique. Il permet également de gérer tout le matériel COMSEC comptable. Comme l'illustre la Figure 1, l'EKMS GC assure ces services à l'appui des communications sécurisées de la voix et des données ainsi que pour l'initialisation des systèmes de génération et de production de clés. Des explications plus détaillées et la doctrine connexe sur l'EKMS GC figurent dans la *Doctrine canadienne en matière de cryptographie visant le Système de gestion électronique des clés du gouvernement du Canada (EKMS GC)* (CCD-06).

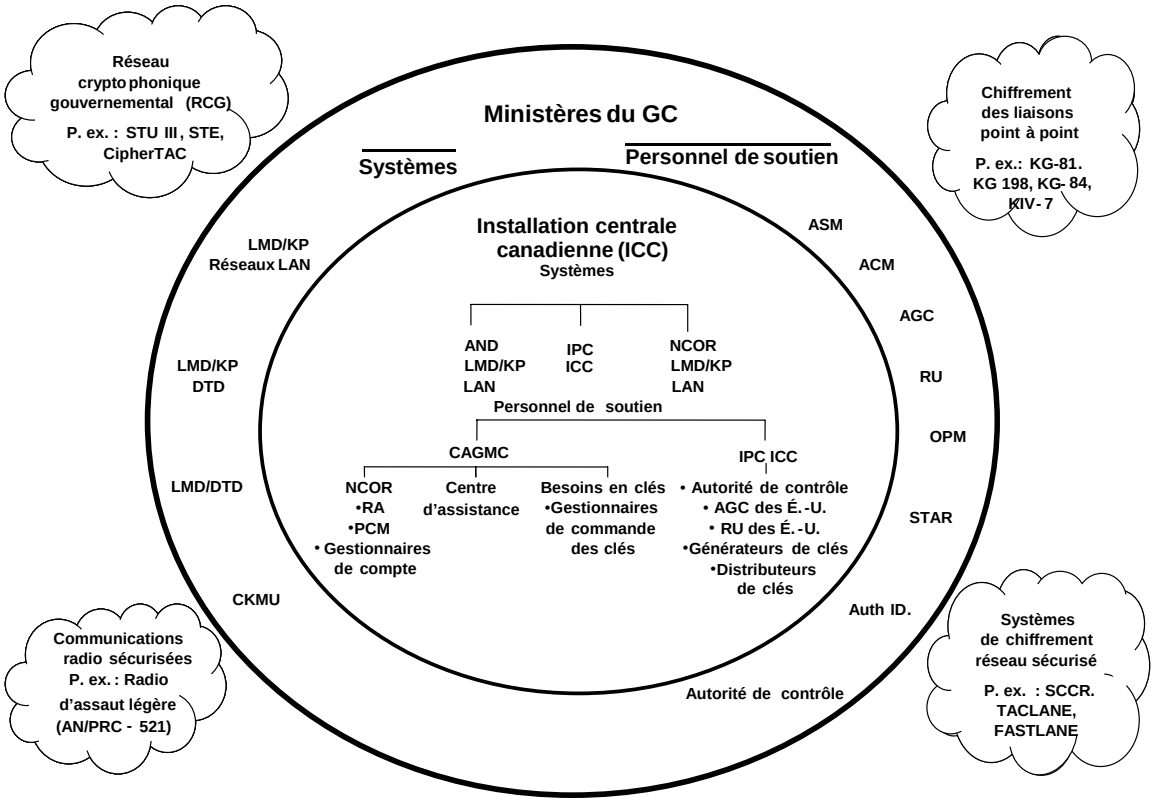

Figure 1 – EKMS GC

2.2.2 Installation centrale canadienne (ICC)

2.2.2.1 Généralités

L'ICC est responsable de la gestion globale de l'EKMS GC et détient les privilèges lui permettant d'accéder à toutes les fonctions racines de l'EKMS GC. L'ICC comprend des systèmes

automatisés et un personnel qui assurent une assistance aux utilisateurs, un soutien opérationnel et l'administration des systèmes.

2.2.2.2 Centre d'assistance et de gestion du matériel cryptographique (CAGMC)

Le CAGMC comprend le Bureau des exigences en matière de matériel cryptographique, le Bureau national des dossiers (NCOR) et le Centre d'assistance, à l'appui de ses activités.

Les responsabilités du Bureau des exigences en matière de matériel cryptographique sont les suivantes :

a. inscrire les autorités de gestion des clés (AGC), les gestionnaires de privilèges de commande (OPM), les représentants des utilisateurs (RU) et les demandeurs d'attribution de titre abrégé (STAR);
b. traiter les demandes d'établissement de privilèges (PER);
c. recevoir et traiter les commandes de clés cryptographiques;
d. établir et tenir à jour les calendriers de livraison pour la distribution des clés cryptographiques.

Les responsabilités du NCOR sont les suivantes :

a. maintenir un inventaire principal du matériel COMSEC comptable, y compris les clés cryptographiques produites ou confiées au Canada;
b. s'assurer que les normes comptables COMSEC minimales, décrites dans le *Manuel de contrôle du matériel COMSEC* (ITSG-10), sont respectées;
c. agir à titre d'autorité d'inscription (RA) nationale pour l'établissement des comptes COMSEC et l'inscription du personnel des comptes;
d. agir à titre de gestionnaire des certificats de privilèges (PCM) pour l'attribution des privilèges au niveau des comptes.

Les responsabilités du Centre d'assistance sont les suivantes :

a. assurer un soutien opérationnel quotidien aux utilisateurs par téléphone, courriel, messagerie vocale, télécopieur et serveur de messagerie EKMS;
b. assurer un service pendant les heures normales de bureau (entre 8 h et 16 h, heure de l'Est). Le Centre d'assistance peut également mettre en œuvre un service de messagerie vocale ou de téléavertisseur ou des heures prolongées pour les périodes en dehors de ces heures, en temps de crise ou encore si les besoins opérationnels l'exigent;
c. offrir un soutien en ligne par l'intermédiaire du site Web du CAGMC : http://www.cse-cst.gc.ca/fr/services/cagmc/cagmc.html;
d. offrir de l'aide pour tous les problèmes de gestion de clés touchant l'EKMS GC.

2.2.2.3 Installation de production de clés de l'Installation centrale canadienne (IPC ICC)

L'IPC ICC joue un rôle majeur dans la génération, la production, la distribution et la comptabilité des clés. Cette installation consiste en systèmes spécialisés pouvant générer et produire les clés nationales, alliées et de l'OTAN.

Les ministères équipés d'un dispositif de gestion locale/processeur de clés (LMD/KP) de l'EKMS GC produiront des clés électroniques traditionnelles pour répondre à leurs propres besoins.

2.2.2.4 Autorité nationale de distribution (AND)

L'AND est le principal intermédiaire en ce qui concerne le matériel COMSEC comptabilisé au niveau national qui entre ou qui sort du Canada. L'AND offre également un soutien pour ce qui est du contrôle de la qualité et de la distribution en vrac des clés produites par l'IPC ICC, s'il y a lieu.

2.3 Clés cryptographiques de l'EKMS GC

2.3.1 Clés traditionnelle et moderne

2.3.1.1 Généralités

Une clé cryptographique est une suite de lettres, de symboles ou de chiffres, un peu comme un très long mot de passe, qu'on utilise conjointement avec un algorithme cryptographique pour contrôler le chiffrement ou le déchiffrement de l'information. La clé est un moyen qui permet non seulement de masquer l'information, mais également de la protéger contre toute modification non autorisée, non détectée ou toute utilisation non autorisée. Outre les fonctions de chiffrement et de déchiffrement, certaines clés permettent également la signature numérique. Le chiffrement assure la confidentialité de l'information, tandis que la signature numérique en assure l'authentification, la non-répudiation et l'intégrité. Il y a deux principaux types de clés : la clé traditionnelle (symétrique) et la clé moderne (asymétrique).

2.3.1.2 Clé traditionnelle (symétrique)

La clé traditionnelle est une clé commune partagée par deux (ou plusieurs) parties pour chiffrer les messages en clair et déchiffrer le texte chiffré. Les parties qui partagent les copies de cette clé commune doivent avoir une confiance mutuelle afin que la clé ne soit pas divulguée et qu'elle soit protégée contre toute modification. La technologie des clés traditionnelles existe depuis longtemps et elle est bien comprise. Elle est relativement rapide et peut traiter des volumes importants de données sans aucune dégradation appréciable. Toutefois, la distribution sûre de cette clé, notamment quand elle est en clair, devient un problème de gestion de clés. La clé doit être en la possession de tous les destinataires prévus, et ceux-ci uniquement, et les destinataires doivent savoir quand l'utiliser. En outre, quand l'utilisation d'une telle clé est requise pour des réseaux de communication entre des utilisateurs qui ne se connaissent pas mutuellement, les risques de compromission du réseau sont plus élevés.

2.3.1.3 Clé moderne (asymétrique)

La clé moderne repose sur le protocole de gestion de clés FIREFLY, qui utilise la cryptographie à clé publique. La clé moderne, ou clé FIREFLY, sert à établir une clé de session entre deux entités. La clé de session générée à partir d'un échange FIREFLY est ensuite utilisée dans un algorithme de chiffrement symétrique. Deux clés initiales distinctes (mathématiquement liées et asymétriques) sont utilisées pour exécuter les fonctions de chiffrement ou de déchiffrement.

Cette paire de clés (aussi appelée biclé) consiste en une clé privée et une clé publique. On peut utiliser l'une ou l'autre clé pour le chiffrement ou le déchiffrement, mais quand l'une d'entre elles a été utilisée pour le chiffrement, l'autre doit servir au déchiffrement.

Les trois types de clés modernes pris en charge par l'ICC sont les suivants :

a. clé STU III;
b. clé de communications SDNS (*Secure Data Network System*);
c. clé de signature de message (MSK).

2.3.2 Identification des clés

2.3.2.1 Généralités

Les clés constituent du matériel COMSEC comptable et, à ce titre, doivent être contrôlées et comptabilisées conformément au *Manuel de contrôle du matériel COMSEC* (ITSG-10). Aux fins d'identification, de contrôle et de suivi, on leur attribue un titre abrégé, une édition, un code de comptabilité (CC), un numéro de comptabilité et une classification de sécurité.

2.3.2.2 Titre abrégé

Un titre abrégé est une méthode non classifiée d'étiquetage du matériel COMSEC afin d'en faciliter la manutention, la comptabilité et le contrôle. Ces titres peuvent se trouver en divers endroits sur le matériel. Les titres abrégés du matériel électronique peuvent être affichés sur les équipements pris en charge par l'EKMS dont, entre autres, le dispositif de transfert des données (DTD), le dispositif de gestion locale (LMD) et le processeur de clés (KP).

Il existe aujourd'hui plusieurs normes nationales différentes sur les titres abrégés. La norme sur les titres abrégés pour l'EKMS sera employée pour tout le matériel cryptographique généré à l'appui des nouveaux systèmes, tandis que le matériel existant, comme les bandes-clés, continuera de recevoir ses titres patrimoniaux jusqu'à ce que les systèmes de production passent à la norme EKMS.

Pour en savoir plus sur les titres abrégés des clés, veuillez consulter le document *Nomenclature des titres abrégés au Canada (ITSG-09).*

Tableau 1 – Exemples de titres abrégés de clés STU III

Titre abrégé de clé STU III canadienne	Type de clé et classification	Méthode de livraison	Type d'équipement
CDNAU 1001	Type 1 Opérationnelle – PROTÉGÉ CRYPTO	Dispositif de stockage de clés	STU III, KOV 14C, STE
CDNAU 1002	Type 1 Opérationnelle – CONFIDENTIEL CRYPTO	Dispositif de stockage de clés	STU III, KOV 14C, STE
CDNAU 1003	Type 1 Opérationnelle – SECRET CRYPTO	Dispositif de stockage de clés	STU III, KOV 14C, STE
CDNAU 1004	Type 1 Opérationnelle – TRÈS SECRET CRYPTO	Dispositif de stockage de clés	STU III, KOV 14C, STE

Titre abrégé de clé STU III canadienne	Type de clé et classification	Méthode de livraison	Type d'équipement
CDNAU 1005	Type 1 Diversification – Toutes classifications	Dispositif de stockage de clés	STU III, KOV 14C, STE
CDGAU 1006	Type 2 Opérationnelle – NON CLASSIFIÉ	Dispositif de stockage de clés	STU III Type 2

Tableau 2 – Exemples de titres abrégés de clés SDNS

Titre abrégé de clé SDNS canadienne	Type de clé et classification	But de la clé	Méthode de livraison	Types d'équipement
CAFAU 2001	Type 1 Opérationnelle – Toutes classifications	Opérationnelle	Dispositif de stockage de clés	SCCR
CAFZU 2002	Type 1 Opérationnelle – NON CLASSIFIÉ CRYPTO	Test		SCCR
CAFZE 3001 845550	Type 1 Opérationnelle – NON CLASSIFIÉ CRYPTO	Test	Dispositif de transfert des données	TACLANE KG 175
CAFZD 3001 845550	Type 1 Opérationnelle – NON CLASSIFIÉ CRYPTO	Test	Transaction chiffrée en vrac	TACLANE KG 175
CAFAD 3002 845550	Type 1 Opérationnelle – Toutes classifications	Opérationnelle	Transaction chiffrée en vrac	TACLANE KG 175
CAFAE 3002 845550	Type 1 Opérationnelle – Toutes classifications	Opérationnelle	Dispositif de transfert des données	TACLANE KG 175

Tableau 3 – Exemples de titres abrégés de clés MSK

Titre abrégé de clé MSK canadienne	Type de clé et classification	But de la clé	Méthode de livraison	Types d'équipement
CAKAU 11111	Type 1 Opérationnelle – Toutes classifications	Opérationnelle	Dispositif de stockage de clés	SCCR
CAKZU 11111	Type 1 Opérationnelle – NON CLASSIFIÉ CRYPTO	Test	Dispositif de stockage de clés	SCCR

Tableau 4 – Exemples de titres abrégés de clés traditionnelles

Titre abrégé de clés traditionnelles canadiennes	Type de clé et classification	But de la clé	Méthode de livraison	Types d'équipement
CSE/537/878	Type 1 Opérationnelle – Toutes classifications	Opérationnelle	Bande-clé	KG 84
CAKZE 2 8455550	Type 1 Opérationnelle – NON CLASSIFIÉ CRYPTO	Test	Dispositif de transfert des données	TACLANE KG 175
CAKZD 2 8455550	Type 1 Opérationnelle – NON CLASSIFIÉ CRYPTO	Test	Transaction chiffrée En vrac	TACLANE KG 175
PC 841000 845999	Certificat – NON CLASSIFIÉ	Opérationnelle	Électronique, par le serveur de messagerie de l'ICC	KOK 22

2.3.2.3 Édition

Un numéro d'édition de clé identifie l'émission d'une série ou d'une version spécifique de matériel COMSEC associée au même titre abrégé. Ce numéro peut être constitué de lettres ou de chiffres. Les clés identifiées par un numéro d'édition sont de durée limitée et sont remplacées par l'édition suivante, quand celle-ci entre en vigueur. La période de validité d'une clé est appelée « fréquence de remplacement ». La fréquence de remplacement d'une clé classifiée possède la cote minimale CONFIDENTIEL, à moins que l'autorité de contrôle (AC) ne lui ait attribué une cote supérieure. La fréquence de remplacement d'une clé désignée PROTÉGÉ possède quant à elle la cote minimale PROTÉGÉ A, à moins que l'autorité de contrôle ne lui ait attribué une cote supérieure.

Pendant un changement de données universelles de clés MSK, SDNS et STU III, soit tous les cinq ans ou à la discrétion de l'ICC, la clé reçue aura deux éditions. Les avis de changement de données universelles sont émis par le CAGMC et transmis aux ministères qui détiennent la ou les clés en cause.

Tableau 5 – Exemples d'édition de matériel cryptographique

Produit	Types d'équipement	Titre abrégé	Édition
Clé STU III	STU III	CDNAU 1005	PD
Période de changement de clé STU III	STU III	CDNAU 1005	PD, PE
Bande-clé	KG 84	CSE 53799	AA
Clé SDNS	KG 175	CAFAD 3002 845550	020001
Clé MSK	KOK 22	CAKAU 11111	000201

2.3.2.4 Segments de clé

Les segments de clé permettent de distinguer les clés individuelles livrées dans une même édition. Chaque segment est identifié de manière unique et le numéro de chaque segment consécutif d'une même édition augmente de un (1). La période de validité d'un segment est appelée « cryptopériode ». La cryptopériode est classifiée de la même manière que la fréquence de remplacement de l'édition, indiquée à la section 2.3.2.3.

2.3.2.5 Code de comptabilité (CC)

Les CC indiquent les contrôles comptables et le signalement requis pour les clés. Le CC d'une clé ne figure habituellement pas sur cette dernière, mais est inclus dans les rapports comptables utilisés par le gardien COMSEC. Le document ITSG-10 contient une description des CC; le lecteur trouvera au chapitre 5 un complément d'information sur les CC pour ce qui est de la commande de clés.

2.3.2.6 Numéro de comptabilité

On attribue à la plupart du matériel COMSEC un numéro de comptabilité unique (numéro de registre, de série ou de copie) au point d'origine afin d'en faciliter la comptabilité. Le numéro de comptabilité des clés traditionnelles est souvent appelé « numéro de registre » (n^o reg.) tandis que le numéro de comptabilité des clés modernes est appelé « numéro d'identification de matériel de chiffrement » (KMID).

2.3.3 Objet des clés cryptographiques

Une clé cryptographique sert essentiellement à six fins :

a. opérationnelle – Si l'ID EKMS autorisé requiert une clé destinée à protéger en ligne des renseignements opérationnels, pour produire des renseignements opérationnels ou pour produire ou sécuriser une transmission électrique de séquences de clés. La classification de la clé comprendra la mention CRYPTO.

b. test – Si l'ID EKMS autorisé requiert une clé destinée à la mise à l'essai en ligne de systèmes ou de l'équipement COMSEC. La classification de la clé comprendra la mention CRYPTO.

c. formation –

   Salle de classe – Si la clé est destinée à la formation en salle de classe en ligne ou hors émission. Si la clé est destinée à la formation en ligne, la classification de la clé comprendra la mention CRYPTO.

   Exercice de formation – Si la clé est destinée à la protection des transmissions associées aux exercices. Si la clé est destinée aux exercices en ligne, la classification de la clé comprendra la mention CRYPTO.

d. maintenance – Si l'ID EKMS autorisé requiert une clé destinée à une utilisation interne hors émission. La classification de la clé ne comprendra pas la mention CRYPTO.

e. développement – Si l'ID EKMS autorisé requiert une clé destinée à la protection du matériel ou de l'équipement COMSEC « en cours » de production. La classification de la clé comprendra la mention CRYPTO.

f. échantillon – Si l'ID EKMS autorisé requiert une clé destinée à des démonstrations hors émission. La classification de la clé peut comprendre la mention CRYPTO.

2.3.4 Sources des clés cryptographiques

Le CST a la responsabilité de fournir aux ministères des clés nationales et/ou étrangères, ou de les autoriser à les générer. L'ICC prend en charge le traitement des commandes de clés pour la génération et la production de tous les types de clés traditionnelles et modernes ainsi que pour l'acquisition de matériel de chiffrement auprès de nations alliées. L'ICC a la capacité de produire des clés pour les distribuer en formats électronique et physique. Les comptes COMSEC pourvus d'un LMD/KP peuvent être autorisés à générer des titres abrégés spécifiques de clés traditionnelles nationales et/ou alliées en format électronique seulement.

2.3.5 Applications des clés cryptographiques

Les systèmes cryptographiques utilisent habituellement des clés traditionnelles (p. ex., clé KG 84) ou des clés modernes (p. ex., clé STU III). Toutefois, certains équipements, comme le TACLANE, peuvent utiliser les clés modernes et traditionnelles pour une même fonction, tandis que d'autres équipements emploient les deux types de clés de manière complémentaire, chacun effectuant une fonction différente. On peut utiliser, par exemple, une clé moderne pour transmettre des clés traditionnelles ou signer des messages.

Les clés cryptographiques peuvent servir aux fins suivantes :

a. chiffrement (liaisons) point à point – Application de la cryptographie en ligne aux liaisons individuelles d'un système de communication, de sorte que toute l'information (y compris les données de routage et d'adressage) transitant par ces liaisons est entièrement chiffrée.

b. chiffrement de bout en bout – Processus dans lequel toutes les données sont chiffrées, de l'expéditeur au destinataire. Bien que les données soient chiffrées quand elles transitent par un réseau, l'information de routage demeure visible.

c. chiffrement de disques et de fichiers – Processus qui consiste à chiffrer l'information enregistrée sur un ordinateur en utilisant des produits de chiffrement/déchiffrement, logiciels ou matériels.

d. téléphone – On peut utiliser des postes téléphoniques spécialisés comme le STU III et l'appareil terminal sécurisé (STE/KOV14C) pour chiffrer les communications voix et données (p. ex., télécopieur).

e. radio – Les radios de campagne utilisées pour les opérations tactiques et stratégiques chiffrent les communications voix et données au sein d'un groupe sélectionné.

f. réseau local (LAN)/réseau étendu (WAN) – Des systèmes de chiffrement réseau, comme le SCCR ou le TACLANE, peuvent être installés pour chiffrer les communications de réseaux entiers.

g. signature numérique – Transformation cryptographique des données qui assure l'authentification d'origine, l'intégrité des données et la non-répudiation du signataire.

2.3.6 Caractéristiques des clés cryptographiques

Les clés peuvent être commandées pour diverses fins (p. ex., opérations, formation, etc.), utilisations (p. ex., FIREFLY), classifications, etc. Le chapitre 5 donne une liste complète des types de commande ainsi que les descriptions connexes.

2.3.6.1 Équipement cryptographique de type 1

Seul l'équipement cryptographique de type 1 et les systèmes qui ont été homologués ou approuvés par le CST doivent être utilisés pour protéger les communications électroniques qui transmettent de l'information classifiée et PROTÉGÉ C. L'équipement cryptographique de type 1, également appelé équipement « de haut niveau », comprend l'équipement COMSEC classifié comme le processeur de clés (KOK 22A) et les articles cryptographiques contrôlés (CCI) comme le STU III, le KG 84 et le TACLANE (KG 75).

2.3.6.2 Équipement cryptographique de type 2

L'équipement cryptographique de type 2, aussi appelé équipement « de bas niveau », comprend l'équipement cryptographique non classifié (p. ex., STU III Type 2) qui a été homologué ou approuvé par le CST. Il peut être utilisé pour protéger les communications électroniques qui transmettent de l'information désignée. On ne doit pas utiliser un équipement cryptographique de type 2 pour protéger de l'information classifiée.

2.4 Processus de gestion des clés

2.4.1 Aperçu

Pour qu'une clé cryptographique soit efficace, elle requiert un processus qui régit le quand et le comment de son utilisation. Ces services de gestion des clés doivent être fournis dès l'introduction d'un nouveau dispositif cryptographique et pendant les phases de commande, de génération, de production, de distribution, de comptabilité, d'utilisation et de destruction de la clé. Les principales activités de gestion des clés sont illustrées à la Figure 2. Les sections subséquentes donnent un bref aperçu du processus de gestion des clés et de la relation entre chaque activité et la commande de clés.

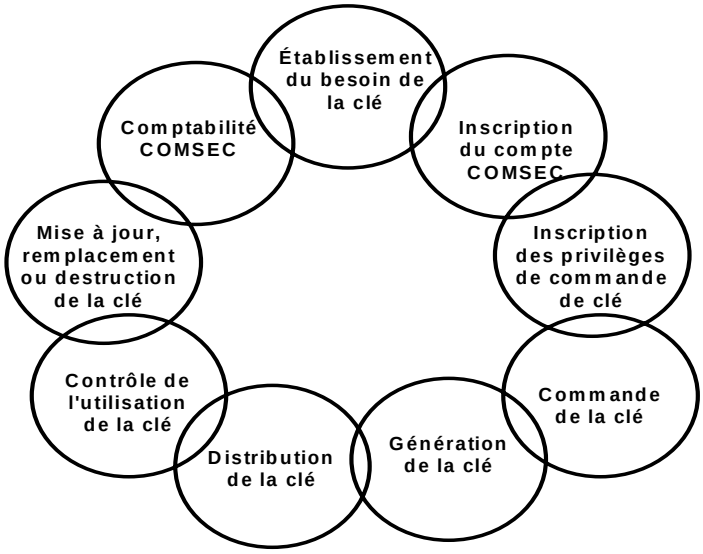
Établissement du besoin de la clé
Inscription du compte COMSEC
Inscription des privilèges de commande de clé
Commande de la clé
Génération de la clé
Distribution de la clé
Contrôle de l'utilisation de la clé
Mise à jour, remplacement ou destruction de la clé
Comptabilité COMSEC

Figure 2 – Fonctions de gestion des clés

2.4.2 Établissement des besoins en communications sécurisées

Quand le ministère a établi un besoin de traiter électroniquement de l'information classifiée ou désignée, il doit communiquer avec le chef des Services à la clientèle de la Sécurité cryptographique au CST. Les consultants du CST offriront des conseils et de l'orientation sur les types d'équipement disponibles et sur les exigences relatives à l'établissement de nouveaux réseaux cryptographiques.

2.4.3 Établissement d'un compte COMSEC

Après l'approbation du chef des Services à la clientèle de la Sécurité cryptographique pour l'obtention d'un équipement cryptographique, le ministère doit communiquer avec le CAGMC pour établir un compte COMSEC afin de superviser le contrôle et le traitement du matériel COMSEC comptable. Ce processus consiste à inscrire l'information sur le compte et à nommer le personnel responsable du compte. Le document ITSG-10 renferme de l'information détaillée au sujet de l'établissement d'un compte COMSEC.

2.4.4 Inscription des privilèges de commande de clés

L'inscription des privilèges de commande de clés comprend :

a. la nomination du personnel du ministère autorisé à commander des clés;

b. l'inscription des privilèges de commande de clés pour un compte EKMS.

2.4.5 Commande de clés

2.4.5.1 Généralités

La présentation d'une commande de clés au CAGMC amorce le processus qui aboutit à la génération de la clé et à son chargement subséquent dans le support prévu (p. ex., papier, KSD, DTD). Le chapitre 5 fournit plus de détails sur la façon de remplir un formulaire de demande de clés.

2.4.5.2 Délai d'exécution

Un délai d'exécution suffisant doit être alloué pour donner le temps à l'IPC ICC de traiter la commande de clés, de planifier la génération de la clé, de générer cette dernière, de la produire et de la livrer avant le moment d'utilisation prévu. Les directives générales, pour ce qui est du délai d'exécution à allouer lors de la présentation d'une commande de clés, sont les suivantes :

a. allouer de deux à trois semaines pour la livraison de tous les types de clé générés par l'ICC;
b. allouer de six à huit semaines pour la livraison de tous les types de clé qui doivent être générés par une installation centrale étrangère.

2.4.5.3 Clés d'urgence

On devrait conserver en tout temps un nombre minimal de clés afin de répondre aux exigences opérationnelles et aux imprévus comme la défaillance de l'équipement, la remise à zéro accidentelle de l'équipement, les clés endommagées, les clés défectueuses ou les clés compromises. Pour déterminer combien de clés d'urgence ou de réserve à stocker, il faut tenir compte du nombre de dispositifs en cours d'utilisation et du temps requis pour se réapprovisionner en clés. La durée de réapprovisionnement dépend du type de clé demandé et de la méthode de livraison. Consultez le document ITSG-10, chapitre 6, pour plus amples renseignements.

2.4.5.4 Génération et production de clés

Le processus de génération est hautement sensible et doit employer de l'équipement approuvé et certifié par le CST. Le CST est autorisé, à titre d'autorité nationale, à générer tous les types de matériel de chiffrement national et de clés étrangères spécifiques. À l'heure actuelle, l'IPC ICC au CST génère la majorité des clés requises par le GC. Quand ils auront été mis en œuvre, les comptes entièrement automatisés et pourvus d'un LMD/KP généreront les clés électroniques traditionnelles si les privilèges appropriés leur ont été accordés. L'IPC ICC continuera d'être la seule entité capable de générer les clés modernes et les clés traditionnelles sur papier.

2.4.5.5 Distribution des clés

Le processus de distribution consiste à transférer une clé de manière sûre de son lieu de génération à l'équipement cryptographique dans lequel elle sera chargée en bout de ligne. L'ICC distribue la clé aux comptes COMSEC selon ce qui est indiqué sur la commande de clés. La clé est ensuite distribuée au sein du compte COMSEC ou à d'autres comptes COMSEC autorisés, suivant les indications de l'autorité de contrôle pour cette clé. L'IPC ICC génère initialement toutes les clés sous forme d'image électronique. Cette image électronique est ensuite convertie

dans le format de livraison spécifié par le type de clé et les exigences de livraison qui figurent sur la commande de clés. L'IPC ICC prend en charge divers mécanismes de livraison, notamment :

a. support papier (bande-clé, carnets);
b. transaction chiffrée en vrac (BET);
c. support magnétique;
d. dispositif de transfert des données (DTD);
e. dispositif de stockage de clés (KSD);
f. carte PCMCIA;
g. remise à la clé électronique.

2.4.6 Contrôle de l'utilisation des clés

Une clé doit être utilisée uniquement dans les conditions spécifiques déterminées par l'autorité de contrôle pour le réseau cryptographique et selon la doctrine opérationnelle appropriée pour le cryptosystème utilisé. Tout écart par rapport à cette procédure pourrait entraîner la compromission de la clé. Entre autres, on ne doit pas utiliser la clé plus longtemps que la cryptopériode spécifiée pour cette clé (c.-à-d. la période pendant laquelle la clé est en vigueur).

2.4.7 Remplacement des clés

Afin de réduire la possibilité que l'information protégée par la clé ne soit compromise, les utilisateurs sont tenus de remplacer la clé conformément à la date d'entrée en vigueur et à la fréquence de remplacement spécifiées dans la commande de clés. Dans certains cas, il faudra détruire physiquement ou remettre à zéro la clé devant être remplacée. Pour plus de détails, consultez le ITSG-10. Les quatre méthodes de remplacement des clés dans l'équipement sont les suivantes :

a. conversion de la clé de diversification – charger la nouvelle clé de diversification et télécharger électroniquement la clé opérationnelle de l'ICC;
b. remise à clé en temps réel – remplacer électroniquement la clé opérationnelle au moyen d'une communication sécurisée avec l'ICC;
c. remise à la clé avec stockage et transmission ultérieure – remplacer électroniquement la clé opérationnelle au moyen de transactions de demande et de réponse avec l'ICC;
d. chargement de la nouvelle clé opérationnelle.

2.4.8 Comptabilité COMSEC

Comme la clé est la partie la plus vulnérable de tout système, elle est assujettie à des procédures de contrôle de matériel COMSEC encore plus rigoureuses que celles qui touchent les autres types de matériel COMSEC. Les clés sont contrôlées et comptabilisées par le Système national de contrôle du matériel COMSEC (SNCMC), depuis leur génération jusqu'à leur destruction. Consultez le ITSG-10 pour plus d'information.

Page intentionnellement laissée en blanc

3 Rôles et responsabilités en matière de commande de clés

3.1 Aperçu

Les rôles relatifs à la commande de clés et les privilèges connexes permettent aux ministères de contrôler et de coordonner l'obtention et l'utilisation des clés requises pour leurs liaisons et systèmes de communications sécurisés. Les rôles et responsabilités en matière de commande de clés diffèrent selon le type de clé et les capacités du compte générateur. Certains privilèges s'appliquent aux clés traditionnelles, et d'autres, uniquement aux clés modernes. Les privilèges de commande ne sont pas universels (en d'autres mots, il n'y a pas de privilège unique qui permette à un compte EKMS de commander n'importe quel titre abrégé). Tous les privilèges de commande sont restreints (p. ex., selon le titre abrégé, le code de partition, le code DAO, le type de clé, la classification de clé, le but de la clé, etc.).

La Figure 3 illustre la hiérarchie des rôles pour la commande de clés traditionnelles et modernes. Les privilèges de chaque compte EKMS qui commande de clés ou demande l'établissement de privilèges de commande de clés doivent être inscrits dans le compte qui générera la clé (p. ex., ICC, LMD/KP).

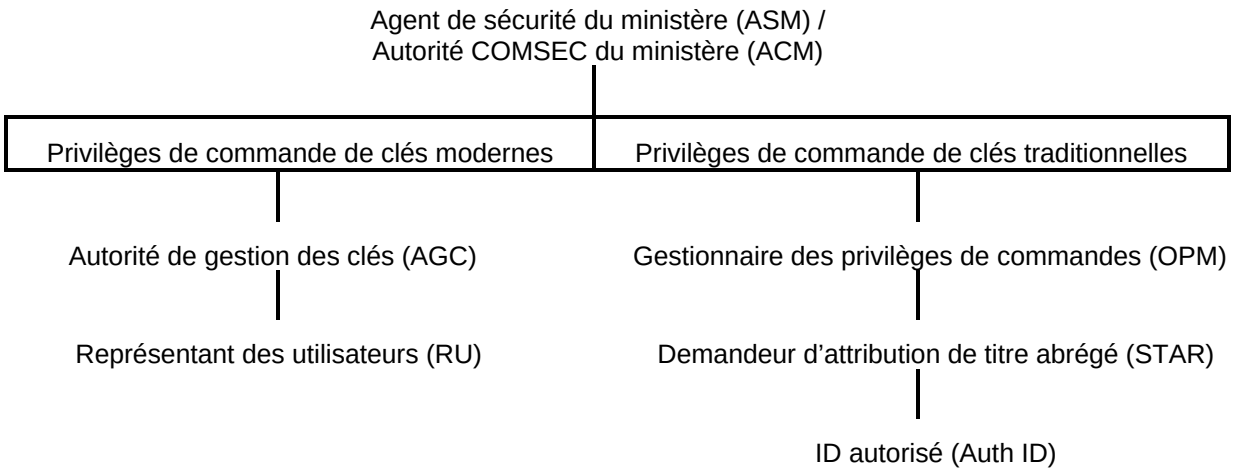
Agent de sécurité du ministère (ASM) /
Autorité COMSEC du ministère (ACM)
Privilèges de commande de clés modernes
Privilèges de commande de clés traditionnelles
Autorité de gestion des clés (AGC)
Gestionnaire des privilèges de commandes (OPM)
Représentant des utilisateurs (RU)
Demandeur d'attribution de titre abrégé (STAR)
ID autorisé (Auth ID)

Figure 3 – Hiérarchie des privilèges de commande

3.2 Agent de sécurité du ministère (ASM)/Autorité COMSEC du ministère (ACM)

Chaque ministère qui commande des clés pour protéger des renseignements classifiés ou désignés de nature extrêmement délicate devrait nommer un ACM qui établira et maintiendra une sécurité efficace des communications au sein du ministère. Dans les petits ministères, l'ACM peut également exécuter plusieurs ou tous les rôles de commande de clés requis par le ministère.

Outre les responsabilités énumérées dans les *Lignes directrices en matière de sécurité des télécommunications au gouvernement du Canada* (ITSD-01), les ACM, ou en l'absence de ceux-ci, les agents de sécurité du ministère (ASM), ont les responsabilités suivantes pour la commande de clés :

a. nommer une nouvelle AGC, un nouvel OPM ou une nouvelle autorité de contrôle, le cas échéant;

b. mettre fin aux fonctions de l'AGC et de l'OPM, le cas échéant;

c. s'assurer que l'AGC et l'OPM reçoivent la formation nécessaire pour l'exécution de leurs tâches.

3.3 Autorité de contrôle

Une autorité de contrôle désignée par l'ASM/ACM est seulement requise quand les réseaux cryptographiques utilisent des clés traditionnelles. Le rôle de l'autorité de contrôle est d'établir et de maintenir l'ordre pour superviser la logistique cryptographique et pour réagir aux questions en matière de sécurité qui ont une incidence sur le réseau cryptographique. L'autorité de contrôle peut également exécuter un, plusieurs ou tous les rôles de commande de clés requis par le ministère. Les responsabilités de l'autorité de contrôle touchent les aspects suivants :

a. le nombre de membres du réseau cryptographique et toute modification apportée à ce nombre;

b. le statut de la clé, y compris la date d'entrée en vigueur de la première édition, les dates d'entrée en vigueur des autres clés, le nombre de segments par édition et toutes les modifications au statut de la clé;

c. le moment du changement de clé dans le réseau cryptographique;

d. l'objet, l'utilisation et le type de la clé requise;

e. la méthode de livraison de la clé;

f. tous les contrôles et restrictions particuliers relatifs à la manutention et à la distribution de la clé;

g. le nombre prescrit de clés de réserve ou d'urgence à commander pour assurer un approvisionnement adéquat advenant des remplacements d'urgence et d'autres événements imprévus;

h. le remplacement de la clé;

i. la promulgation de l'information sur le statut de la clé;

j. l'élaboration et la gestion des plans de gestion des clés.

NOTE : Une autorité de contrôle peut uniquement superviser des clés propres au ministère.

3.4 Privilèges de commande de clés traditionnelles

3.4.1 Gestionnaire des privilèges de commande (OPM)

L'OPM est nommé par l'ASM ou l'ACM par la présentation d'un certificat de nomination à l'ICC. L'OPM a la responsabilité d'inscrire auprès de l'ICC les privilèges OPM et STAR pour un compte EKMS. Au niveau supérieur de la hiérarchie, l'OPM est :

a. autorisé à effectuer toutes les fonctions de commande associées aux privilèges OPM, STAR et Auth ID;
b. responsable de la sélection des personnes et de la demande des privilèges OPM et STAR pour le compte EKMS, auprès de l'ICC;
c. responsable de la formation en matière de commande de clés, par l'intermédiaire du Centre de formation STI du CST;
d. responsable de la mise en œuvre de la doctrine nationale touchant toutes les activités relatives à la gestion de clés traditionnelles, au sein de son ministère, et de la promulgation de toute directive additionnelle ou explicative.

3.4.2 Demandeur d'attribution de titre abrégé (STAR)

Le STAR est nommé par l'OPM sur présentation d'un certificat de nomination à l'ICC. L'OPM doit déjà être inscrit auprès de l'ICC. Le STAR a la responsabilité de présenter des commandes au CAGMC pour créer de nouveaux titres abrégés et accorder le privilège Auth ID (ID autorisé) à des ID EKMS pour ces titres abrégés. Le cas échéant, le STAR peut exécuter toutes les fonctions associées à un ID autorisé.

3.4.3 ID autorisé (Auth ID)

Le privilège Auth ID (ou ID autorisé) est attribué par le STAR, l'OPM ou un autre ID autorisé, au moyen de la présentation d'une PER pour clés traditionnelles. À l'ICC, le privilège Auth ID permet à son détenteur de présenter des commandes de clés traditionnelles pour :

a. lancer la génération d'une clé pour un titre abrégé spécifique;
b. spécifier/modifier le profil de distribution pour un titre abrégé spécifique;
c. octroyer ou révoquer le privilège Auth ID des autres comptes pour un titre abrégé spécifique;
d. demander la modification des attributs d'un titre abrégé spécifique;
e. annuler le titre abrégé.

3.5 Privilèges de commande de clés modernes

3.5.1 Autorité de gestion des clés (AGC)

L'AGC est nommée par l'ACM. Le rôle de l'AGC est normalement attribué à un fonctionnaire supérieur œuvrant dans le domaine de la sécurité ou de la COMSEC. Plusieurs AGC peuvent être nommées dans les grands ministères. Le cas échéant, les domaines de responsabilité de chaque AGC doivent être clairement délimités afin d'éviter tout chevauchement. Dans les petits ministères, l'ACM peut également décider de jouer le rôle d'AGC.

Les principales responsabilités de l'AGC comprennent :

a. la sélection et l'inscription des représentants des utilisateurs qui ont la permission de commander des clés modernes auprès de l'ICC;
b. l'inscription des privilèges de commande de clés pour chaque représentant d'utilisateur, y compris l'établissement des descriptions DAO (ministère, agence, organisme) pour lesquelles le représentant des utilisateurs aura l'autorité de commander des clés;

c. la formation des représentants des utilisateurs, par l'intermédiaire du Centre de formation STI du CST;

d. la mise en œuvre d'une doctrine nationale pour toutes les activités touchant la gestion des clés modernes au sein du ministère et la promulgation de toute directive additionnelle ou explicative.

3.5.2 Représentant des utilisateurs (RU)

Le représentant des utilisateurs (RU) est sélectionné et inscrit auprès de l'ICC par l'AGC. Le nombre de personnes sélectionnées par l'AGC pour assumer ce rôle dépend de la structure du ministère, de l'emplacement de ses installations et de ses préoccupations en matière de sécurité. La fonction RU est normalement attribuée à une personne qui a des responsabilités en matière de sécurité et/ou de COMSEC au sein du ministère. Le représentant des utilisateurs doit être un citoyen canadien, mais il ne doit pas nécessairement avoir une cote de sécurité pour commander des clés, à moins qu'il ne doive accéder à de l'information classifiée (p. ex., date d'entrée en vigueur). Le RU est responsable des activités suivantes :

a. interagir avec les utilisateurs pour déterminer leurs besoins en matière de clés en fonction des nouveaux équipements, des changements apportés à l'information d'identification ou de la remise à la clé d'un équipement;

b. vérifier que les utilisateurs ont les cotes de sécurité requises pour le niveau de classification des clés qu'ils commandent;

c. préparer et présenter les commandes de clés au CAGMC;

d. interagir avec le personnel du CAGMC afin de surveiller l'état des commandes de clés;

e. interagir avec le gardien COMSEC pour l'aviser de toute clé attendue.

3.6 Privilèges de commande de clés américaines

3.6.1 Généralités

L'ICC est inscrite auprès de la *U.S. Central Facility* (Installation centrale américaine), de la même manière que tous les ministères du GC sont inscrits auprès de l'ICC.

3.6.2 *U.S. Command Authority* (Autorité de commande américaine)

La *U.S. Command Authority* à l'ICC est désignée par l'ACM du CST. Elle a la responsabilité de nommer des représentants des utilisateurs et d'inscrire leurs privilèges auprès de la *U.S. Central Facility*.

NOTE : La *U.S. Command Authority* est l'équivalent américain de l'AGC.

3.6.3 Représentant des utilisateurs américains

Le représentant des utilisateurs américains valide toutes les commandes de clés américaines provenant des ministères du GC et soumet ces commandes à la *U.S. Central Facility* en vue de leur traitement et de la génération des clés. Les ministères du GC qui présentent de telles commandes doivent avoir des privilèges de commande de clés américaines inscrits auprès du CAGMC.

4 Inscription et gestion des privilèges

4.1 Généralités

La commande de clés comporte trois étapes : l'inscription, l'établissement des privilèges et la commande. Ces trois étapes sont définies ci-dessous. La Figure 4 illustre le processus d'inscription et d'établissement de privilèges pour les clés modernes. Les Figure 5 à 8 présentent une ventilation des processus d'inscription et de gestion des privilèges illustrés à la Figure 4.

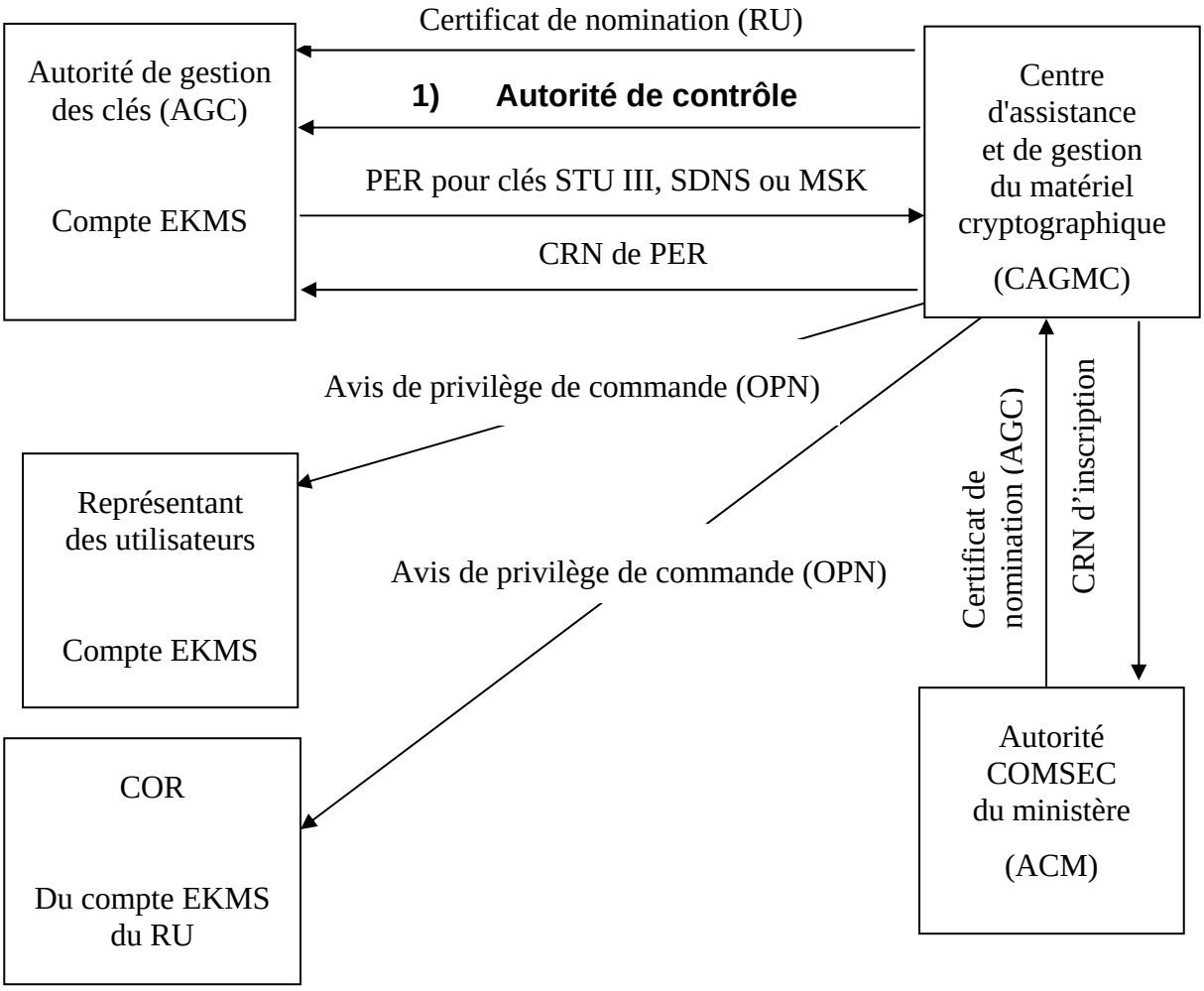
Certificat de nomination (RU)
Autorité de gestion des clés (AGC)
1) Autorité de contrôle
Centre d'assistance et de gestion du matériel cryptographique (CAGMC)
PER pour clés STU III, SDNS ou MSK
Compte EKMS
CRN de PER
Avis de privilège de commande (OPN)
Certificat de nomination (AGC)
CRN d'inscription
Représentant des utilisateurs
Compte EKMS
Avis de privilège de commande (OPN)
COR
Du compte EKMS du RU
Autorité COMSEC du ministère (ACM)

Figure 4 – Inscription des privilèges de commande de clés modernes

4.1.1 Inscription

L'inscription est le processus qui permet à des personnes d'assumer certaines responsabilités de gestion des clés au sein d'un compte. L'inscription d'un compte s'effectue avec le formulaire Inscription d'un compte tandis que l'inscription d'une personne se fait avec le formulaire Certificat de nomination.

Inscription des AGC et des OPM

L'ASM ou l'ACM présente un Certificat de nomination pour inscrire les AGC et les OPM auprès du CAGMC. Le CAGMC répond par un Accusé d'inscription.

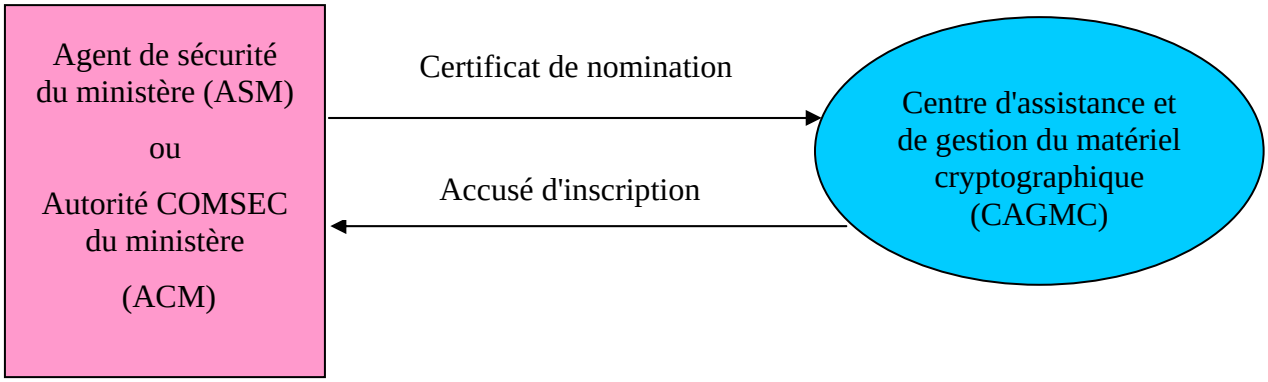

Figure 5 – Inscription des AGC/OPM

Inscription des représentants des utilisateurs et des STAR

L'AGC présente un Certificat de nomination pour inscrire les représentants des utilisateurs (RU) et l'OPM présente un Certificat de nomination pour inscrire les STAR auprès du CAGMC. Le CAGMC répond par un Accusé d'inscription.

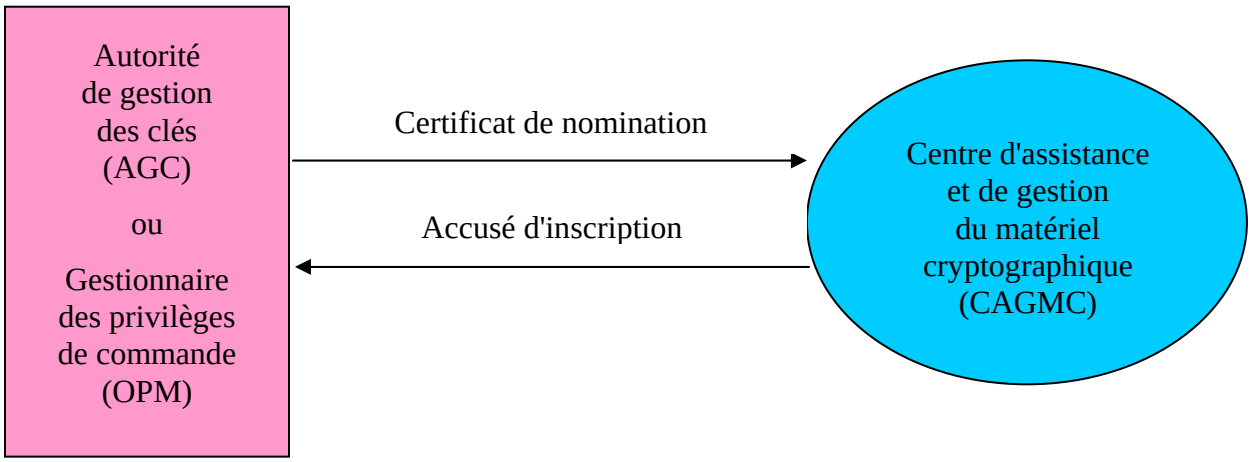
Autorité de gestion des clés (AGC)
ou
Gestionnaire des privilèges de commande (OPM)
Certificat de nomination
Accusé d'inscription
Centre d'assistance et de gestion du matériel cryptographique (CAGMC)

Figure 6 – Inscription des RU/STAR

4.1.2 Gestion des privilèges

La gestion des privilèges est le processus qui consiste à attribuer, tenir à jour et appliquer les contrôles d'accès pour les personnes et les comptes. Le processus d'octroi, de modification ou de révocation des privilèges de gestion des clés s'effectue au moyen d'une demande d'établissement de privilèges (PER).

L'AGC présente une PER pour clés SDNS, MSK ou STU III afin de demander des privilèges de commande de clés auprès du CAGMC pour l'ID EKMS. L'OPM présente une PER pour clés traditionnelles afin de demander des privilèges STAR au CAGMC pour l'ID EKMS. Le CAGMC répondra à chaque PER en envoyant un CRN de PER pour indiquer si la PER a été approuvée ou rejetée. Le CRN de PER est envoyé à l'ID EKMS qui a présenté la demande PER.

Gestion des privilèges – PER rejetée par le CAGMC

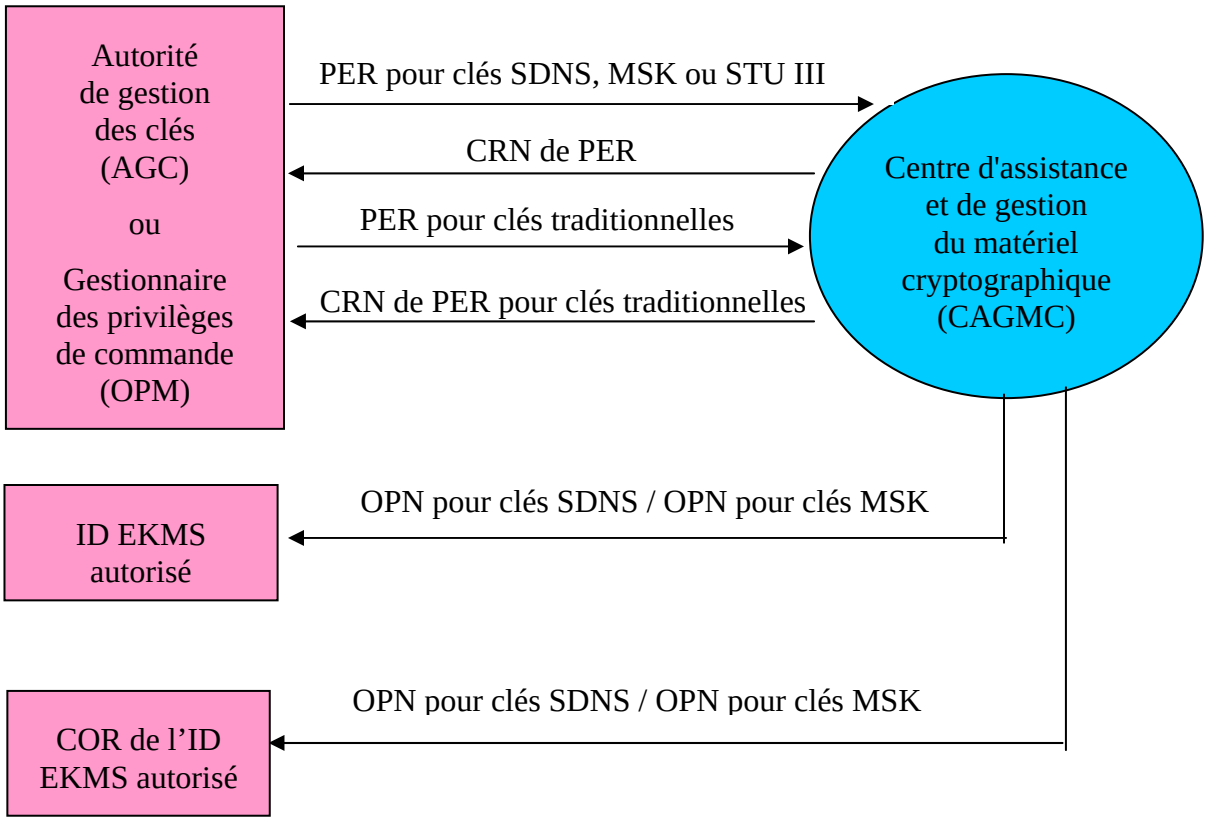
Autorité de gestion des clés (AGC)
ou
Gestionnaire des privilèges de commande (OPM)
PER pour clés SDNS, MSK ou STU III
CRN de PER
PER pour clés traditionnelles
CRN de PER pour clés traditionnelles
Centre d'assistance et de gestion du matériel cryptographique (CAGMC)
ID EKMS autorisé
OPN pour clés SDNS / OPN pour clés MSK
COR de l'ID EKMS autorisé
OPN pour clés SDNS / OPN pour clés MSK

Figure 7 – Gestion des privilèges – PER rejetée par le CAGMC

NOTE : Les OPN pour clés STU III ne sont pas envoyés du CAGMC à l'ID EKMS autorisé ni au COR de l'ID EKMS autorisé.

4.1.3 Commande de clés

La commande de clés est le processus qui consiste à lancer la production des clés et à les livrer à un compte COMSEC autorisé à les recevoir. Le processus de commande de clés s'effectue à l'aide du formulaire Demande de clés.

L'ID EKMS autorisé présente une commande de clés SDNS, MSK, traditionnelle ou STU III au CAGMC. La commande de clés est ensuite approuvée ou rejetée, d'après les privilèges attribués à cet ID EKMS. Le CAGMC répondra à chaque commande de clés par l'envoi d'un CRN de commande.

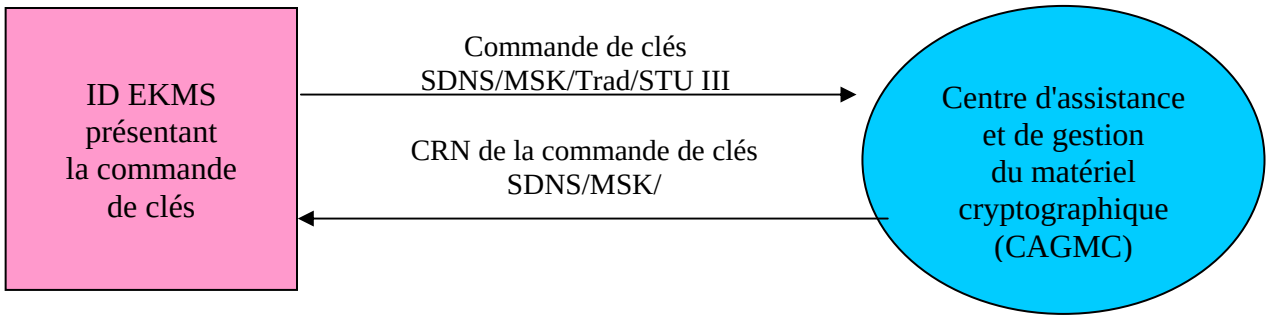
ID EKMS présentant la commande de clés
Commande de clés SDNS/MSK/Trad/STU III
CRN de la commande de clés SDNS/MSK/
Centre d'assistance et de gestion du matériel cryptographique (CAGMC)

Figure 8 – Processus de commande de clés

4.2 Formulaires et avis

Le Tableau 6 indique les formulaires et avis utilisés pour l'inscription du personnel affecté à la commande de clés et de leurs privilèges. Les annexes indiquées dans le tableau contiennent des exemples de ces formulaires et avis. Bon nombre des cases, sur ces formulaires, se passent d'explications. Une brève explication des autres cases figure aux sections indiquées et sur les formulaires.

Il est important que toutes les sections des formulaires soient entièrement lisibles afin que le personnel du CAGMC puisse traiter correctement l'information. Une information inexacte pourrait se traduire par une identification incorrecte de l'utilisateur ou par des commandes de clés invalides. Les formulaires remplis sont envoyés au CAGMC.

Tableau 6 – Formulaires de demande d'inscription et de gestion de privilèges

Formulaire/avis	Description/utilisation	Exemple de formulaire	Explications à la section
Certificat de nomination	Indique toute l'information requise pour nommer le personnel ministériel autorisé à commander des clés ou pour révoquer leur nomination.	Annexe C	4.3
Demande d'établissement de privilèges (PER) pour clés STU III	Indique toute l'information requise pour ajouter, remplacer ou supprimer des codes DAO (ministère, agence, organisme), des descriptions DAO et les attributs associés à un code DAO.	Annexe D	4.4
Demande d'établissement de privilèges (PER) pour clés SDNS	Indique toute l'information requise pour ajouter, remplacer ou supprimer des privilèges de commande de clés SDNS à un ID EKMS.	Annexe E	4.5
Demande d'établissement de privilèges (PER) pour clés MSK	Indique toute l'information requise pour ajouter ou supprimer des privilèges de commande de clés MSK à un ID EKMS.	Annexe F	4.6
Demande d'établissement de privilèges (PER) pour clés traditionnelles	Indique toute l'information requise pour ajouter, remplacer ou annuler des privilèges de commande OPM ou STAR associés à un ID EKMS.	Annexe G	4.7
Avis de confirmation/rejet de la PER (CRN de PER)	Indique les privilèges octroyés ou révoqués, en réponse à une PER pour clés traditionnelles, STU III, SDNS ou MSK.	Annexe H	4.8

Formulaire/avis	Description/utilisation	Exemple de formulaire	Explications à la section
Avis de privilège de commande (OPN)	Indique les privilèges OPM, STAR ou RU octroyés par l'ID EKMS générateur (ICC) à un autre ID EKMS en réponse à une PER approuvée pour clés traditionnelles, SDNS ou MSK.	Annexe I	4.9

4.3 Certificat de nomination

4.3.1 Généralités

Le Certificat de nomination, à l'Annexe C, sert à nommer des personnes ou à révoquer la nomination de personnes autorisées à commander des clés ou à attribuer des privilèges de commande à un compte EKMS.

4.3.2 Nouvelle nomination

4.3.2.1 Autorisation

Le personnel assumant les rôles suivants doit être officiellement nommé à ce titre :

- L'ASM nomme l'ACM.
- L'ASM/ACM nomme l'AGC et l'OPM.
- L'AGC nomme les représentants des utilisateurs (RU) et les RU suppléants.
- L'OPM nomme les STAR.

La personne qui autorise la nomination doit s'assurer que la personne désignée :

a. possède la citoyenneté canadienne;

b. a obtenu une habilitation de sécurité d'un niveau comparable au niveau de sensibilité le plus élevé de l'information ou du matériel auquel cette personne aura accès;

c. a assisté à une séance d'initiation COMSEC si elle doit manipuler physiquement la clé (en d'autres mots, le gardien COMSEC, le gardien suppléant, l'utilisateur final, etc.);

d. a pris connaissance de toutes les tâches et responsabilités liées au poste.

4.3.2.2 Habilitation de sécurité

À moins qu'elle ne manipule physiquement la clé (en d'autres mots, le gardien COMSEC, le gardien COMSEC suppléant, l'utilisateur final), la personne nommée n'a pas besoin d'avoir une habilitation de sécurité plus élevée que la clé qu'elle est autorisée à commander.

4.3.2.3 Formation du personnel

Avant sa nomination, ou dans les trois mois suivant sa nomination, chaque personne appelée à jouer le rôle AGC, RU, OPM ou STAR doit assister à un cours officiel sur la commande de clés cryptographiques. Les gardiens COMSEC, les ASM et les ACM sont également invités à assister

à ce cours. On peut obtenir du Centre de formation STI du CST le calendrier des cours et de l'information sur l'inscription.

L'ACM ou le personnel actuellement nommé pour commander les clés devrait fournir une formation provisoire afin de s'assurer que chaque personne nommée comprend bien les procédures d'attribution de privilèges et de commande de clés. Si cette formation provisoire ne s'offre pas au ministère de la personne nommée, elle peut être fournie par le CAGMC.

4.3.3 Changement de personnel

La personne qui autorise la nouvelle nomination doit présenter un Certificat de nomination pour la nouvelle personne nommée et doit remplir la section Cessation des fonctions sur une copie du Certificat de nomination original pour la personne qui est remplacée. Le changement de personnel devra être effectué avant le départ de la personne actuellement nommée.

4.4 Formulaire Demande d'établissement de privilèges (PER) pour clés STU III

4.4.1 Généralités

La PER pour clés STU III, à l'Annexe D, est utilisée par l'AGC pour inscrire les privilèges de commande de clés pour le représentant des utilisateurs STU III nommé au compte EKMS. Le formulaire indique les privilèges du représentant des utilisateurs STU III pour des codes DAO et des descriptions DAO spécifiques pour lesquels le RU peut commander une clé. Le formulaire indique également les types de clé autorisés et la classification maximale de la clé.

4.4.2 Type de demande

Le formulaire est utilisé pour ajouter, modifier ou supprimer un ou plusieurs codes DAO et leurs attributs connexes. Les changements doivent être envoyés au CAGMC rapidement pour tenir les dossiers à jour et permettre l'attribution et l'envoi des nouveaux codes DAO au représentant des utilisateurs approprié.

Les actions ci-dessus sont décrites ci-après :

a. ajout : un privilège STU III est ajouté à l'ID EKMS. Le CAGMC attribuera le code DAO.
b. modif. : un privilège STU III existant est modifié. On doit fournir le code DAO qui sera modifié.
c. suppr. : tous les privilèges de commande de clés STU III associés au code DAO spécifié seront supprimés. On doit fournir le code DAO qui sera supprimé.

4.4.3 Code DAO

Quand vous ajoutez une nouvelle description DAO, n'inscrivez rien dans la case Code DAO. Le CAGMC attribuera un code DAO de six chiffres à la description DAO. Ce code sera transmis à l'AGC et au représentant des utilisateurs par l'intermédiaire de l'Avis de confirmation/rejet de la PER pour clés STU III (anciennement appelé Formulaire d'autorisation de commande de clés). Les codes DAO sont utilisés par le représentant des utilisateurs pour commander des clés. Quand on modifie ou on supprime une description DAO, et/ou les attributs connexes, on doit entrer le code DAO attribué. Chaque code DAO sera attribué à un seul représentant des utilisateurs, mais

un représentant des utilisateurs peut se voir attribuer plusieurs codes DAO. La description DAO doit contenir au plus 16 caractères (y compris les espaces) et correspond à une ligne d'affichage sur le poste STU III.

4.4.4 Description DAO

4.4.4.1 Généralités

L'identification de l'utilisateur est un élément essentiel de la clé STU III. Elle est affichée sur le poste STU III distant quand un appel sécurisé est établi. Chaque identification d'utilisateur comporte deux parties : une description DAO et une case de données d'identification additionnelles (à structure libre). Il incombe à l'AGC d'indiquer la description DAO, tandis qu'il revient au représentant des utilisateurs de remplir la case de données d'identification additionnelles. Le représentant des utilisateurs fournira les données d'identification additionnelles sur le formulaire Demande de clés STU III (voir l'article 5.2.10).

4.4.4.2 Ligne 1

La ligne 1 de la description DAO est obligatoire. Cette première ligne est affichée sur le poste distant pendant la durée de chaque appel sécurisé. Il devrait s'agir de la description bilingue (facultative pour les clés étrangères), reconnaissable et commune du ministère, plutôt qu'une abréviation énigmatique ou un désignateur numérique qui ne serait pas facilement reconnu par les personnes qui communiquent avec ce poste STU III. Les sigles reconnus dans l'ensemble du gouvernement, comme DND/MDN, GRC/RCMP et CSE/CST, sont acceptables. Chaque ligne doit contenir au plus 16 caractères (y compris les espaces), ce qui correspond à une ligne d'affichage sur le poste STU III.

4.4.4.3 Ligne 2

La ligne 2 de la description DAO est facultative. Elle sera affichée momentanément sur le poste distant pendant l'établissement de l'appel sécurisé. Cette deuxième ligne devrait être utilisée par l'AGC pour inscrire de l'information additionnelle décrivant le DAO, comme un désignateur d'emplacement, de section, d'unité ou de poste. Par ailleurs, on peut laisser cette case en blanc. Cela laisse donc deux lignes disponibles, utilisables pour des données additionnelles d'identification. La deuxième ligne ne doit pas servir à inscrire des noms de personnes.

4.4.4.4 Règles pour les descriptions DAO

Les règles pour l'identification de la description DAO sont les suivantes :

a. la première ligne de la description DAO doit indiquer le DAO du parrain ou d'une partie importante de celui-ci, ou d'un sous-traitant du gouvernement;
b. le ministère indiqué dans la description DAO doit être représentatif du DAO pour lequel l'AGC est nommée;
c. chaque description DAO doit être unique non seulement dans le ministère, mais également dans tous les ministères;
d. chaque description DAO peut être inscrite et utilisée par un représentant des utilisateurs;

e. chaque ligne peut contenir jusqu'à 16 caractères, y compris les espaces. Les caractères valides sont les lettres majuscules (A à Z), les chiffres (0 à 9) et les caractères spéciaux suivants :

, . / [ ] ! “ # $ % & ‘ ( ) + - = ; < > ?

f. on ne peut pas utiliser les caractères accentués (É, È, À, etc.), l'astérisque (*) et la barre oblique inverse (\) dans une description DAO;

g. la description DAO devrait être affichée en format bilingue;

h. la ligne 2 de la description DAO pour la clé STU III utilisée doit contenir l'ID EKMS du compte pour les communications entre des comptes EKMS équipés d'un LMD ou d'un LMD/KP;

i. les descriptions DAO peuvent uniquement être créées, modifiées et supprimées par l'AGC.

4.4.5 Indicateur d'utilisation EKMS

Une clé identifiée pour utilisation EKMS peut être utilisée uniquement par le compte EKMS pour lequel elle est autorisée. La clé EKMS STU III est requise aux fins d'authentification pendant les communications directes entre des comptes EKMS entièrement et/ou partiellement automatisés et pour les communications électroniques avec l'ICC.

La clé EKMS STU III peut être utilisée par le personnel du compte EKMS pour les communications classifiées autres que les communications EKMS. Quand la clé STU III est utilisée pour des communications non EKMS, le LMD doit être déconnecté et mis hors tension.

4.4.6 Demande de privilèges de commande pour d'autres comptes EKMS

Un compte peut demander des privilèges de commande pour d'autres comptes EKMS.

4.4.7 Type de clé autorisée

4.4.7.1 Généralités

Le type de clé comprend le niveau du type de clé, lequel désigne le niveau le plus élevé de protection assuré par la clé, et le statut opérationnel de celle-ci.

4.4.7.2 Niveau du type de clé

Il y a deux niveaux possibles de types de clé pour la clé STU III :

a. Le type 1 désigne une clé autorisée à protéger l'information classifiée, non classifiée et protégée. Une clé de type 1 peut uniquement être utilisée dans de l'équipement de type 1.

b. Le type 2 désigne les clés autorisées à protéger l'information jusqu'au niveau PROTÉGÉ B inclusivement. Une clé de type 2 peut uniquement être utilisée dans un équipement de type 2.

4.4.7.3 Indicateur de clé opérationnelle /diversification

On distingue les clés opérationnelles des clés de diversification d'après le type d'information électronique enregistré dans le mécanisme de livraison (c.-à-d. KSD). Une clé opérationnelle peut être utilisée pour sécuriser les communications dès son chargement dans l'équipement de

destination, tandis qu'une clé de diversification doit être convertie en clé opérationnelle avant que l'on puisse débuter les communications sécurisées (c.-à-d. remise à la clé électronique). L'utilisateur amorce cette conversion en téléphonant à l'ICC au (613) 991-8600. Pendant cet appel, la clé de diversification dans l'équipement de destination est convertie en clé opérationnelle.

On peut se procurer une clé opérationnelle pour le STU III de type 1 et de type 2 ainsi que les cartes cryptographiques KOV 14C. Les clés de diversification sont disponibles uniquement pour les terminaux STU III de type 1.

L'AGC doit indiquer tous les types de clés qui peuvent être commandés par le représentant des utilisateurs STU III pour chaque code DAO et description DAO.

4.4.7.4 Clé STU III américaine

S'il faut communiquer avec des organismes américains sur le réseau STU III américain, l'AGC doit obtenir l'autorisation du CAGMC pour commander une clé nationale américaine. Pour obtenir cette autorisation, l'AGC doit présenter une explication écrite du besoin, indiquer les personnes américaines et canadiennes en cause et la nature des discussions qui auront lieu. Le CAGMC examinera la demande et déterminera si l'autorisation sera accordée. Les commandes de clés nationales américaines ne seront pas traitées par le CAGMC si cette autorisation n'est pas accordée. Les privilèges de commande de clés américaines doivent être rattachées à des codes DAO, à des descriptions DAO et à des RU spécifiques.

4.4.8 Classification maximale de la clé

Sélectionnez la classification maximale de la clé que le représentant des utilisateurs peut commander pour chaque code DAO selon les directives suivantes :

a. la seule classification valide pour les clés opérationnelles de type 2 est NON CLASSIFIÉ, ce qui comprend les désignations PROTÉGÉ A et B;
b. la classification maximale pour la clé STU III avec le code 25 de Classe 6 (Mobile, c.-à-d. utilisable dans un CipherTAC) est SECRET;
c. la classification maximale sélectionnée doit être égale ou supérieure à la classification la plus élevée du ou des codes de Classe 6 sélectionnés.

4.4.9 Codes de Classe 6

Lors de la commande de clés, le représentant des utilisateurs doit préciser ses besoins en matière de clés de Classe 6. Il existe actuellement six codes de Classe 6 :

Code	Message affiché
01	PROTECTC
02	PROTECTB
03	PROTECTA
10	SCI
20	US
99	TEST

Le code 10 (clé SCI TRÈS SECRET) de Classe 6 est destiné à être utilisé dans les zones approuvées pour la discussion ou le traitement de renseignements cloisonnés de nature délicate (SCI). Cette description ne s'affiche que si elle est associée à la clé des deux postes en communication. Toutes les autres descriptions de code de Classe 6 s'affichent pourvu que l'un des deux postes soit muni d'une clé assortie au code en question.

Au fur et à mesure que de nouveaux codes de Classe 6 seront disponibles, on les annoncera et on fera parvenir aux utilisateurs de STU III les instructions régissant leur usage.

4.5 Formulaire de demande d'établissement de privilèges (PER) pour clés SDNS

4.5.1 Généralités

La PER pour clés SDNS, à l'Annexe E, est utilisée par l'AGC afin d'inscrire les privilèges de commande de clés pour les RU actuellement nommés au compte EKMS. Le formulaire indique les privilèges du RU pour les codes de partition spécifiques parmi lesquels le RU peut commander des clés. Il indique également les types de clé et les types d'équipement associés au code de partition. Une fois remplis, les formulaires PER pour clés SDNS sont présentés au CAGMC.

4.5.2 Type de demande

On utilise le formulaire pour ajouter ou supprimer un ou plusieurs codes de partition et leurs attributs connexes. Les changements doivent être envoyés rapidement au CAGMC pour tenir à jour les dossiers et permettre l'attribution et l'envoi des nouveaux codes de partition au RU approprié.

Les actions ci-dessus sont décrites ci-après :

a. ajout : un privilège pour clés SDNS sera ajouté à l'ID EKMS;

b. suppression : tous les privilèges SDNS qui ont la combinaison indiquée d'ID EKMS et de codes de partition seront supprimés.

4.5.3 Demande de privilèges de commande pour d'autres ID EKMS

Un compte peut demander des privilèges de commande pour d'autres comptes EKMS.

4.5.4 Code de partition

Les privilèges de partition ouverte permettent aux RU de commander des clés SDNS pour des utilisateurs qui veulent communiquer avec tous les autres abonnés de la partition ouverte. Une partition ouverte est similaire au RCG, en ce sens qu'aucun abonné n'est exclu du réseau de communication.

Les privilèges de partition fermée permettent aux RU de commander des clés SDNS pour un ensemble donné d'utilisateurs, selon ce qu'aura déterminé l'administrateur du réseau et/ou l'autorité de contrôle, qui détermine qui peut communiquer dans le réseau. Les partitions fermées peuvent être isolées davantage à l'intérieur des réseaux au moyen de contrôles d'accès.

Les codes de partition seront approuvés par le chef des Services à la clientèle de la Sécurité cryptographique, et attribués par le CAGMC.

4.5.5 Type de clé autorisée

4.5.5.1 Généralités

Le type de clé comprend le niveau du type de clé, lequel indique le niveau maximal de protection offerte par la clé, ainsi que le statut opérationnel de celle-ci.

4.5.5.2 Niveau du type de clés

Il y a deux niveaux possibles de type de clés SDNS :

a. la clé de type 0 sert à générer une clé de chiffrement de clés (KEK), que l'on peut utiliser pour chiffrer en vrac des clés. La clé de type 0 peut être utilisée uniquement avec un KP (KOK 22A);
b. La clé de type 1 désigne une clé dont l'utilisation est autorisée pour protéger l'information classifiée, non classifiée et protégée.

4.5.5.3 Indicateur de clé opérationnelle/diversification

On distingue les clés opérationnelles des clés de diversification d'après le type d'information électronique enregistré dans le mécanisme de livraison (c.-à-d. KSD, DTD). La clé opérationnelle peut être utilisée pour sécuriser les communications dès son chargement dans l'équipement de destination, tandis que la clé de diversification doit être convertie en clé opérationnelle avant que l'on puisse débuter les communications sécurisées (c.-à-d. remise à la clé électronique). L'utilisateur amorce cette conversion en téléphonant à l'ICC et, pendant cet appel, la clé de diversification dans l'équipement de destination est convertie en clé opérationnelle.

NOTE : La clé de diversification et la remise à la clé électronique pour les clés SNDS ne sont actuellement pas disponibles à l'ICC.

4.5.5.4 Classification maximale de la clé

La classification maximale de la clé ne doit pas être supérieure au niveau de classification du compte recevant les privilèges, ni à la classification maximale autorisée par la doctrine régissant l'équipement en cause.

4.5.5.5 Clé SDNS étrangère

Si des communications initiales sont requises avec des entités étrangères, l'AGC doit obtenir l'autorisation du chef des Services à la clientèle de la Sécurité cryptographique pour commander la clé étrangère. Pour obtenir l'autorisation, l'AGC doit présenter une explication écrite du besoin, indiquer les organismes canadiens et étrangers participants et donner la nature de l'information qui sera échangée. Le chef des Services à la clientèle de la Sécurité cryptographique du CST examinera la demande et déterminera si l'autorisation sera accordée. Les commandes de clés étrangères ne seront pas traitées par le CAGMC tant que l'autorisation

n'aura pas été accordée. Les privilèges de commande de clés étrangères doivent être rattachés à des codes de partition spécifiques. Les clés étrangères peuvent comprendre :

a. les clés étrangères;
b. les clés de coalition;
c. les clés CCEB;
d. les clés de l'OTAN;
e. les clés alliées.

NOTE : La remise à la clé pour le SDNS est disponible auprès de la *U.S. Central Facility* pour certains dispositifs. Communiquez avec le CAGMC pour obtenir plus d'information.

4.5.6 But de la clé

Le but de la clé indique la fonction de la clé, comme suit :

a. opérationnelle – Si l'ID EKMS autorisé requiert une clé destinée à protéger en direct des renseignements opérationnels ou pour produire et sécuriser une transmission électrique de flots de clés. La classification de la clé comprendra la mention CRYPTO;
b. test – Si l'ID EKMS autorisé requiert une clé destinée à la mise à l'essai en direct de systèmes ou de l'équipement COMSEC. La classification de la clé comprendra la mention CRYPTO;
c. Formation :
    1) salle de classe – Si la clé est destinée à la formation en salle de classe en direct ou hors émission. Si la clé est destinée à la formation en ligne, la classification de la clé comprendra la mention CRYPTO;
    2) exercice de formation – Si la clé est destinée à la protection des transmissions associées aux exercices. Si la clé est destinée aux exercices en direct, la classification de la clé comprendra la mention CRYPTO.
d. maintenance – Si l'ID EKMS autorisé requiert une clé destinée à une utilisation interne hors émission. La classification de la clé ne comprendra pas la mention CRYPTO;
e. développement – Si l'ID EKMS autorisé requiert une clé destinée à la protection du matériel ou de l'équipement COMSEC « en cours » de production. La classification de la clé comprendra la mention CRYPTO;
f. échantillon – Si l'ID EKMS autorisé requiert une clé destinée à des démonstrations hors émission. La classification de la clé peut comprendre la mention CRYPTO.

4.6 Formulaire Demande d'établissement de privilèges (PER) pour clés MSK

La PER pour clés MSK, à l'Annexe F, est utilisée par l'AGC afin d'inscrire les privilèges de commande de clés pour les représentants des utilisateurs de clés MSK, qui sont actuellement nommés au compte EKMS. L'AGC peut ajouter ou supprimer les privilèges de commande de clés MSK canadiennes ou américaines qui seront utilisées dans un KP (c.-à-d. KOK 22A) en mode opérationnel ou test.

4.6.1 Demande de privilèges de commande pour d'autres ID EKMS

Un compte peut demander des privilèges de commande pour d'autres comptes EKMS.

4.6.2 Type de demande

Ce formulaire sert à ajouter ou supprimer un ou plusieurs privilèges de commande de clés MSK. Les changements doivent être envoyés au CAGMC rapidement dans le but de tenir à jour les dossiers.

Les actions ci-dessus sont décrites ci-après :

a. ajout : un privilège MSK sera ajouté à l'ID EKMS;

b. suppression : tous les privilèges MSK qui ont la combinaison spécifiée d'ID EKMS et de codes DAO seront supprimés.

4.7 Formulaire Demande d'établissement de privilèges (PER) pour clés traditionnelles

La PER pour clés traditionnelles, à l'Annexe G, est utilisée par l'ACM pour inscrire les privilèges de commande de clés OPM et STAR, auprès de l'ICC, pour son ministère. Le formulaire est utilisé pour ajouter ou annuler les privilèges OPM et STAR comme suit :

a. l'action initiale permet à l'ACM d'ajouter des privilèges OPM ou STAR;

b. l'action d'annulation permet à l'ASM/ACM de supprimer le privilège OPM ou STAR.

4.8 Avis de confirmation/rejet de PER (CRN de PER)

L'ICC génère un CRN de PER pour le compte EKMS qui présente la demande, en réponse au traitement de chaque PER. Cet avis confirme ou rejette les privilèges de commande demandés. Toute modification présentée sur une PER donnera lieu à la production d'un nouvel Avis de confirmation/rejet de PER. Un exemple d'Avis de confirmation/rejet de PER figure à l'Annexe H.

4.9 Avis de privilège de commande (OPN)

L'ICC génère un OPN pour le compte EKMS autorisé et pour le COR du compte autorisé, en réponse au traitement de chaque PER. L'OPN indique les privilèges de commande OPM, STAR ou RU qui sont octroyés, révoqués ou modifiés par un compte générateur à un autre compte EKMS en réponse à une PER pour clés traditionnelles, STU III, SDNS ou MSK. Un exemple d'OPN figure à l'Annexe I.

Page intentionnellement laissée en blanc

5 Commande de clés

5.1 Processus de commande de clés

5.1.1 Aperçu

Une commande de clés amorce le processus qui aboutit à la génération et à la distribution d'une clé. Les commandes de clés sont présentées au CAGMC sous diverses formes : par la poste, par messager, par télécopieur protégé ou non et par le serveur de messagerie EKMS de l'ICC. Après que le CAGMC ait traité la commande de clés, un Avis de confirmation/rejet de la commande (CRN de commande) sera envoyé au compte EKMS qui a présenté la commande. Si la commande de clés ne peut pas être traitée (p. ex., si elle n'est pas signée ou s'il manque de l'information), le CAGMC communiquera avec le ministère par téléphone.

5.1.2 Interaction avec les utilisateurs afin de déterminer leurs besoins en matière de clés

Les besoins des utilisateurs peuvent être divers. Ils peuvent vouloir commander des clés pour :

a. doter d'une clé un équipement qui vient d'être acquis et installé;
b. remettre un équipement en service après sa remise à zéro (p. ex., clé opérationnelle effacée pour faciliter la maintenance ou les réparations);
c. changer l'information d'identification à la suite d'une réorganisation, etc.;
d. effectuer des tests ou de la maintenance sur un équipement;
e. remplacer une clé expirée dans des circonstances où la remise à la clé électronique est impossible.

5.1.3 Validation de l'information de sécurité

Le personnel qui commande les clés (p. ex., RU, OPM, STAR) doit certifier, par les voies ministérielles appropriées, que l'utilisateur possède une habilitation de sécurité égale ou supérieure à la classification de la clé demandée. Si la demande n'est pas valide, la commande de clés ne doit pas être transmise au CAGMC.

5.1.4 Préparation de la commande de clés

Le Tableau 7 indique les formulaires et avis de demande de clé qui figurent dans les annexes. L'explication des cases sur les différents formulaires figure aux sections indiquées et sur les formulaires eux-mêmes. Il est important de remplir lisiblement toutes les sections des formulaires pour que le personnel du CAGMC puisse traiter correctement l'information. Une information incorrecte peut donner lieu à une identification d'utilisateur incorrecte ou invalider la demande de clé.

Tableau 7 – Formulaires et avis de commande de clés

Formulaire de demande de clés/ avis	Description/utilisation	Exemple de formulaire	Section explicative
Demande de clés STU III	Sert à commander une clé de diversification ou une clé opérationnelle pour un STU III, un CipherTAC ou un KOV 14C.	Annexe J	5.2
Demande de clés SDNS	Sert à commander une clé FIREFLY pour l'équipement SDNS.	Annexe K	5.3
Demande de clés MSK	Sert à commander une clé de signature de message pour le processeur de clés (KP).	Annexe L	5.4
Demande de clés traditionnelles	Sert à commander une bande-clé physique ou une clé pré-placée KG-175 TACLANE.	Annexe M	5.5
Avis de confirmation/ rejet de la commande (CRN de commande)	Sert à aviser le compte EKMS qui présente la commande de l'état de chaque article commandé.	Annexe N	5.6
Avis de privilège de commande (OPN)	Sert à aviser le compte EKMS qu'il est autorisé à commander la clé pour le compte nommé dans l'OPN.	Annexe I	4.9

5.1.5 Présentation d'une demande de clé

La présentation d'une demande de clé doit tenir compte du temps requis pour générer, produire et distribuer la clé (voir également la section 2.4.5.2). Par ailleurs, le niveau de sensibilité dictera la méthode de transmission de la demande de clé au CAGMC, à savoir :

a. x.400 EKMS;
b. serveur de messagerie;
c. courrier de première classe;
d. messagerie;
e. télécopieur sécurisé ou non sécurisé;
f. téléphone sécurisé ou non sécurisé.

5.1.6 Classification/protection d'une demande de clé

La demande de clé peut être classifiée ou protégée selon son contenu. Chaque formulaire est accompagné d'instructions spécifiques.

5.1.7 Validation d'une demande de clé

Avant de traiter une demande de clé, le CAGMC la valide en fonction des privilèges de commande inscrits de la manière décrite au chapitre 4. Une fois la demande approuvée, un CRN de commande sera généré et transmis au compte EKMS ayant présenté la demande. Le représentant des utilisateurs, l'OPM ou le STAR doit vérifier que le CRN de commande reflète exactement la clé demandée. Le CRN de commande indiquera l'état de chaque élément commandé (p. ex., approuvé ou rejeté). Si un article est approuvé, l'ICC procèdera alors à la production et à la livraison de la clé. Si un article est rejeté, le motif sera fourni au demandeur, et

une nouvelle demande de clé devra être présentée. Si un CRN de commande est reçu pour une commande qui n'a pas été présentée par le compte EKMS ou s'il y a des anomalies dans la demande, le représentant des utilisateurs, l'OPM, le STAR ou le gardien doit appeler le CAGMC sur-le-champ.

5.1.8 Surveillance de l'état de la demande de clé

Le CRN de commande contiendra un ID de transaction de commande. On devrait faire référence à cet ID de transaction quand on communique avec le CAGMC pour demander de l'information au sujet de l'état de la commande.

5.1.9 Avis aux gardiens COMSEC

Les gardiens COMSEC qui recevront la clé doivent être avisés de la commande. La meilleure façon de les aviser consiste, pour le représentant des utilisateurs, l'OPM ou le STAR, de transmettre au gardien COMSEC du compte EKMS qui recevra la clé une copie de la demande de clé et du CRN de commande. Ainsi, le gardien COMSEC pourra vérifier que la clé reçue correspond bien à ce qui a été commandé.

5.2 Formulaire Demande de clé STU III

5.2.1 Généralités

Le formulaire Demande de clé STU III, à l'Annexe J, est utilisé par le représentant des utilisateurs pour commander les clés STU III de type 1 et de type 2.

5.2.2 Numéro de transaction EKMS

Chaque demande de clé doit contenir un identificateur appelé « Numéro de transaction ». Le format de ce numéro est AAMMXXXX, où AA représente les deux derniers chiffres de l'année, MM le mois et XXXX le numéro ascendant selon le mois en cours, qui débute à 0001 chaque mois. Par exemple, 01080005 correspond à la cinquième demande de clé présentée par ce représentant des utilisateurs au cours du mois d'août 2001. Cette case doit comporter en tout huit chiffres. On ne peut utiliser aucun caractère alphabétique.

5.2.3 Type de clé

5.2.3.1 Généralités

Le type de clé comprend le niveau du type de clé, qui désigne le niveau maximal de protection fourni par la clé ainsi que le statut opérationnel de celle-ci.

5.2.3.2 Niveau du type de clé

Les types possibles de clé STU III sont les suivants :

a. le type 1 désigne une clé dont l'utilisation est autorisée pour protéger l'information classifiée, non classifiée et protégée. Une clé de type 1 peut être utilisée uniquement avec de l'équipement de type 1;

b. Le type 2 désigne une clé dont l'utilisation est autorisée pour protéger l'information jusqu'au niveau PROTÉGÉ B inclusivement. Une clé de type 2 peut être utilisée uniquement avec de l'équipement de type 2.

5.2.3.3 Indicateur de clé opérationnelle/diversification

On distingue une clé opérationnelle d'une clé de diversification d'après le type d'information électronique enregistré dans le mécanisme de livraison (c.-à-d. KSD). Une clé opérationnelle peut être utilisée pour sécuriser les communications dès son chargement dans l'équipement de destination, tandis que la clé de diversification doit être convertie en clé opérationnelle avant que l'on puisse débuter les communications sécurisées (c.-à-d. remise à la clé électronique). L'utilisateur amorce cette conversion en téléphonant à l'ICC, et pendant cet appel, la clé de diversification dans l'équipement de destination est convertie en clé opérationnelle.

On peut se procurer une clé opérationnelle pour le STU III de type 1 et le STU III de type 2, le CipherTAC 2000 et les cartes cryptographiques KOV 14C. Les clés de diversification sont disponibles uniquement pour les terminaux STU III de type 1.

Une clé opérationnelle permet à un utilisateur de faire un appel sécurisé sans qu'elle doive être convertie; par conséquent, elle est plus vulnérable à la compromission qu'une clé de diversification. Pour cette raison, on ne devrait commander que des clés de diversification, sauf dans des circonstances spéciales (p. ex., besoin d'une clé d'urgence) dans votre ministère.

5.2.4 Commande de clés STU III EKMS

Les comptes automatisés qui exigent une connexion avec le serveur de messagerie de l'ICC doivent commander une clé STU III. L'ID EKMS du compte où la clé STU III EKMS sera utilisée doit être indiqué pour chaque ligne d'article applicable.

5.2.5 Mécanisme de livraison

La clé STU III est livrée sur KSD 64A ou par remise à la clé électronique. La clé STU III peut être chargée dans les types d'équipement suivants :

5.2.5.1 STU III (y compris le CipherTAC 2000)

La clé de diversification et la clé opérationnelle sont toutes deux disponibles pour être utilisées dans tous les terminaux STU III autres que le CipherTAC 2000, tel qu'indiqué ci-dessus. Le CipherTAC 2000 utilise uniquement la clé opérationnelle provenant d'un KSD. Cette clé est chargée directement dans le CipherTAC 2000 à l'ICC. Ceci comprend la mise à la clé initiale, de même que la remise à la clé, car il n'y a pas de fonctionnalités de remise à la clé électronique pour le CipherTAC 2000. On peut commander une clé STU III pour un ou plusieurs CipherTAC 2000 sur le même formulaire de demande. Le numéro de série du CipherTAC 2000 doit être inclus dans la colonne des observations pour chaque ligne d'article désignée par le code 25 (Mobile) de Classe 6. Vous devez communiquer avec le CAGMC lors du chargement des CipherTAC 2000 afin de prendre des dispositions.

NOTE : Pour en savoir plus sur le CipherTAC 2000, veuillez consulter le document *Doctrine canadienne en matière de cryptographie visant le CipherTAC 2000* (CCD-04).

5.2.5.2 Appareil terminal sécurisé (STE)

La clé STU III destinée à être utilisée avec le STE est chargée directement dans la carte cryptographique KOV 14C à l'ICC. On peut commander une clé STU III pour un ou plusieurs KOV 14C sur le même formulaire de demande. Le numéro de série du KOV 14C doit figurer dans la case 13 du formulaire Demande de clé STU III (colonne des observations), pour chaque ligne d'article applicable. Le formulaire Demande de clé STU III rempli et le formulaire connexe Demande de clé SDNS, s'il y a lieu, doivent être envoyés au CAGMC, alors que la ou les cartes KOV 14C mises à zéro doivent être envoyées à l'AND de l'ICC par l'intermédiaire du SNCMC. Pour en savoir plus sur la carte STE/KOV 14C, veuillez consulter le document *Doctrine canadienne en matière de cryptographie visant la carte cryptographique FORTEZZA PLUS (KOV 14C) et l'appareil téléphonique sûr (STE)* (CCD-11).

NOTE : Pour en savoir plus sur le STU III et les KSD, veuillez consulter les documents *Plan de gestion des clés STU III* (CID/01/13) et le *Manuel d'exploitation du STU III* (MG-7).

5.2.6 Classification de la clé

Entrez la classification et la désignation de la clé pour chaque article. Prenez note des restrictions suivantes :

a. la clé peut avoir une désignation ou une classification allant jusqu'à la classification maximale que le représentant des utilisateurs peut commander pour le code DAO et la description DAO spécifiés pour chaque ligne d'article;

b. si la désignation PROTÉGÉ est indiquée, le code de Classe 6 approprié doit être inclus;

c. la seule classification valide pour une clé opérationnelle de Type 2 est NON CLASSIFIÉ;

d. la classification maximale pour une clé STU III avec le code 25 de Classe 6 (Mobile, c.-à-d. utilisable dans un CipherTAC) est SECRET;

e. la classification maximale sélectionnée doit être égale ou supérieure à la classification maximale du ou des codes de Classe 6 sélectionnés.

5.2.7 Code de Classe 6

Entrez le code de Classe 6, s'il y a lieu. Certains utilisateurs ont besoin d'information d'authentification additionnelle, notamment pour ce qui est de la classification des renseignements cloisonnés de nature délicate. Cela peut être indiqué par l'utilisation des codes de Classe 6. Chaque code de Classe 6 se voit attribuer un numéro de deux chiffres par le CAGMC. Les codes de Classe 6 sont décrits à la section 4.4.9 de la présente publication.

5.2.8 Code DAO

Entrez le code DAO approprié pour chaque clé commandée. Les codes DAO qu'un compte EKMS est autorisé à demander sont indiqués sur le formulaire Autorisation de commander des clés accordée à un représentant des utilisateurs de STU III. Les clés commandées à l'aide d'un code DAO particulier contiennent automatiquement la description associée à ce code. Reportez-vous également à la section 4.4.4 pour en savoir plus.

5.2.9 Données d'identification additionnelles

5.2.9.1 Description

Les données d'identification additionnelles (c.-à-d., zone de texte libre) consistent en deux lignes additionnelles, autre que la description DAO existante pour la clé. Ces données sont affichées sur le STU III, juste après l'affichage de la description DAO. Chaque ligne de données d'identification peut contenir jusqu'à 16 caractères, y compris les espaces, mais la somme des quatre (4) lignes ne doit pas dépasser 50 caractères. La case des données d'identification additionnelles permet de personnaliser la clé d'un ministère, selon des sous-éléments et des utilisateurs spécifiques. Par exemple, on peut indiquer un emplacement géographique ou le titre d'un poste, mais on ne doit pas inclure le nom d’une personne. Les données d'identification additionnelles sont facultatives. Voici un exemple d'identification complète d'utilisateur, avec des descriptions DAO et des données d'identification additionnelles :

Ligne 1	HEALTH CANADA	Description DAO
Ligne 2	SANTE CANADA	Description DAO
Ligne 3	DIR. SECURITE	Texte libre
Ligne 4	OTTAWA	Texte libre

5.2.10 Observations

Il s'agit d'une case facultative dans laquelle vous indiquez toute instruction spéciale, comme les demandes d'expédition spéciales ou l'urgence de la commande.

5.3 Formulaire Demande de clé SDNS

5.3.1 Généralités

Le formulaire Demande de clé SDNS, à l’Annexe K, est utilisé par le représentant des utilisateurs pour commander une clé SDNS canadienne ou américaine pour un type d'équipement spécifié.

NOTE : Le représentant des utilisateurs doit avoir les privilèges de commande de clé SDNS spécifiques auprès de l'ICC pour pouvoir présenter un formulaire de Demande de clé SDNS.

5.3.2 Numéro de transaction

Chaque formulaire de Demande de clé SDNS doit contenir un identificateur appelé « ID de la transaction ». Celui-ci consiste en l'ID EKMS qui présente la commande, la date (AAAAMMJJ)

à laquelle la commande est générée et un numéro ascendant selon le mois en cours, qui recommence à 1 chaque mois.

5.3.3 Code de partition

Sélectionnez « Ouvert » ou « Fermé » pour la clé commandée. On peut indiquer un seul type de partition par clé commandée. Si vous sélectionnez « Fermé », entrez alors un code de partition à 10 chiffres précédemment inscrit par l'AGC. Les codes de partition sont décrits à la section 4.5.4 de la présente publication.

5.3.4 Type d'équipement

Sélectionnez le type d'équipement dans lequel la clé sera utilisée. Sélectionnez un seul type d'équipement par commande de clé. Si le type d'équipement est KP (KOK 22A), l'ID EKMS du compte qui l'utilisera doit être entré pour chaque clé commandée.

5.3.5 Type de clé

5.3.5.1 Généralités

5.3.5.2 Niveau du type de clé

Les types de clé SDNS possibles sont les suivants :

a. la clé de type 0. Elle sert à générer une clé de chiffrement de clés (KEK) que l'on peut utiliser pour chiffrer en vrac des clés en vue de leur distribution. Le seul type d'équipement valide pour la clé de type 0 est le KP (KOK 22A);
b. la clé de type 1. Elle est utilisée pour désigner une clé dont l'utilisation est autorisée pour protéger l'information classifiée jusqu'au niveau TRÈS SECRET inclusivement. Elle est utilisée uniquement dans l'équipement de type 1.

5.3.5.3 Indicateur de clé opérationnelle/diversification

On distingue une clé opérationnelle d’une clé de diversification d'après le type d'information électronique qui est enregistré dans le mécanisme de livraison (c.-à-d. KSD, DTD). Une clé opérationnelle peut être utilisée pour sécuriser les communications dès son chargement dans l'équipement de destination, tandis que la clé de diversification doit être convertie en clé opérationnelle avant que l'on puisse débuter les communications sécurisées (c.-à-d. remise à la clé électronique). L'utilisateur amorce cette conversion en téléphonant à l'ICC, et pendant cet appel, la clé de diversification dans l'équipement de destination est convertie en clé opérationnelle.

NOTE : Les clés de diversification et la remise à la clé électronique pour le SDNS ne sont pas disponibles à l’ICC à l’heure actuelle. La *U.S. Central Facility* peut prendre en charge la remise à la clé électronique pour la plupart des dispositifs SDNS.

5.3.6 Contrôle d'accès

Choisissez « Aucun » si la fonction n'est pas nécessaire. Choisissez « COMMS » si la clé est de type 1 opérationnelle. Choisissez « Distribution » si la clé est de type 0 opérationnelle (LMD/KP).

NOTE : L'option « Distribution » doit être utilisée pour les clés commandées en vue de l'exploitation du LMD/KP. L'option « Aucun » doit être utilisée pour tous les autres types de clés SDNS.

5.3.7 ID ASCII

On peut entrer dans cette case toute information d'identification additionnelle pour chaque clé, comme l'information en texte libre de 14 caractères qui figure sur l'affichage du SCCR.

Les données d'ID ASCII et d'ID ASCII authentifié offrent de l'information lisible par l'utilisateur relativement au contrôle d'accès et à l'identification. Cette information peut décrire un réseau, un compte ou un utilisateur. Les données sont contenues dans la clé et comportent au plus 32 caractères.

L'ID ASCII est utilisé pour la commande d'une clé SCCR. Les représentants des utilisateurs qui commandent cette clé doivent fournir l'ID ASCII approprié au CAGMC.

On utilise l'ID ASCII authentifié pour commander une clé STE/KOV 14C. Les représentants des utilisateurs qui commandent la clé doivent fournir au CAGMC un code DAO inscrit et le descripteur DAO connexe, dans le format approprié. Si un nouveau code DAO et un nouveau descripteur DAO sont requis, l'autorité de gestion des clés STU III du compte doit remplir et présenter une Demande d'établissement de privilèges (PER) pour les clés STU III au CAGMC (voir l'article 4.4). Le CAGMC répondra à la demande en retournant le formulaire Autorisation de commander des clés accordées à un représentant des utilisateurs de STU III.

5.3.8 Mécanisme de livraison

5.3.8.1 Transaction chiffrée en vrac (BET)

Ce mécanisme de livraison est utilisé pour distribuer électroniquement la clé SDNS et ses attributs connexes ainsi que les rapports de comptabilité. Seuls les comptes équipés d'un LMD/KP peuvent recevoir la clé par le mécanisme de livraison BET. À l'heure actuelle, une transaction BET peut prendre en charge 16 clés SDNS au maximum. Le code de comptabilité (CC) pour des clés livrées dans une transaction BET peut être CC 6 ou CC 7.

5.3.8.2 Dispositif de transfert des données (DTD)

Le DTD est un dispositif de remplissage conçu pour stocker, transporter et transférer de manière sûre les clés par voie électronique. À l'heure actuelle, un DTD peut prendre en charge 22 clés SDNS au maximum pendant les périodes de changement de données non universelles, et 11 clés SDNS au maximum pendant les périodes de changement de données universelles. Consultez la doctrine spécifique à votre équipement pour déterminer s'il peut être rempli à l'aide d'un DTD. Pour en savoir plus sur le DTD, consultez le document *Doctrine canadienne en matière de cryptographie visant le dispositif de transfert de données AN/CYZ-10/10A* (CCD-01).

NOTE : Quand on commande des clés qui seront chargées dans un DTD, le représentant des utilisateurs doit aviser l'ICC de la cryptopériode préférée pour la clé de chiffrement de la clé de transfert (TrKEK) de DTD (c.-à-d. base trimestrielle ou annuelle).

5.3.8.3 Dispositif de stockage de clés (KSD)

Le KSD est désigné comme dispositif de remplissage quand il contient une clé opérationnelle ou de diversification. Les seuls CC valides pour la clé SDNS livrée sur un KSD sont CC 1 ou CC 4.

5.3.8.4 KOV 14C

Une clé SDNS utilisée avec le STE est chargée directement dans la carte cryptographique KOV 14C à l'ICC. On peut demander une clé SDNS pour une ou plusieurs cartes KOV 14C sur le même formulaire de commande. Le numéro de série du KOV 14C doit figurer dans la colonne « Observations » pour chaque ligne d'article applicable. Le formulaire Demande de clé SDNS et le formulaire Demande de clé STU III connexe, s'il y a lieu, doivent être envoyés au CAGMC. Les cartes KOV 14C mises à zéro doivent être envoyées à l'ADN par l'intermédiaire du SNCMC. Vous devez inscrire le numéro de transaction de la Demande de clé STU III associée dans la colonne « Observations de la Demande de clé SDNS », pour faire le lien entre les commandes.

NOTE : Pour en savoir plus sur le dispositif STE/KOV 14C, consultez la doctrine CCD-11.

5.4 Formulaire Demande de clé MSK

5.4.1 Généralités

Le formulaire Demande de clé MSK, à l'Annexe L, est utilisé par le RU pour commander une clé MSK canadienne ou américaine pour le KP.

5.4.2 ID de la transaction

Chaque commande de clé MSK doit contenir un identificateur appelé « ID de la transaction ». Cet ID comprend l'ID EKMS qui présente la commande, la date (AAAMMJJ) à laquelle la commande est générée et un numéro ascendant recommençant à un (1) au début de chaque année civile.

5.4.3 Type de clé

Les seuls types de clé MSK valides sont la clé opérationnelle canadienne de type 1 et la clé opérationnelle américaine de type 1. Ces clés sont toujours livrées dans un KSD en tant qu'article CC 1 ou CC 4.

5.4.4 Indicateur d'utilisation EKMS

L'indicateur d'utilisation EKMS indique si la clé est utilisée à l'appui des transactions EKMS seulement. Une clé désignée pour utilisation avec EKMS peut uniquement être utilisée par le compte pour lequel elle est autorisée. À l'heure actuelle, les seules clés MSK utilisées au Canada sont associées à l'EKMS.

5.4.5 ID additionnels

Les cases « ID additionnels » (en texte à structure libre) comprennent l'ID EKMS du compte qui utilisera la clé MSK, suivi d'un deux points (:) et de l'ID EKMS du gestionnaire des certificats de privilèges. L'ID EKMS du gestionnaire des certificats de privilèges pour les ministères du GC autres que le DCOR du MDN est 845999. L'ID EKMS du gestionnaire des certificats de privilèges pour le DCOR du MDN est 844111.

5.5 Formulaire Demande de clés traditionnelles

5.5.1 Généralités

Le formulaire Demande de clés traditionnelles, à l'Annexe M, est utilisé par le STAR ou l'ID autorisé pour commander des clés traditionnelles canadiennes ou américaines pour un type d'équipement précis.

Les articles 5.5.3, 5.5.5, 5.5.6, 5.5.7, 5.5.10, 5.5.11 et 5.5.12 traitent spécifiquement des comptes LCMS partiellement automatisés.

5.5.2 Numéro de la transaction

Chaque Demande de clé traditionnelle doit contenir un identificateur appelé « ID de la transaction ». Cet ID comprend l'ID EKMS qui présente la commande, la date (AAAMMJJ) à laquelle la commande est générée et un numéro ascendant recommençant à 1 au début de chaque année civile.

5.5.3 Types de commande

5.5.3.1 Demande d'attribution de titre abrégé

Le STAR crée une Demande d'attribution de titre abrégé afin d'attribuer un nouveau titre abrégé à un réseau cryptographique, de fournir les attributs du titre abrégé et d'inscrire les ID EKMS autorisés (Auth ID) à présenter des commandes pour ce titre abrégé. L'information contenue dans les cases A, B et D doit être complète.

5.5.3.2 Commande de génération

L'ID autorisé (Auth ID) crée une Demande de génération pour amorcer la génération et la distribution d'un titre abrégé spécifique de clé. L'ID EKMS pour l'ID autorisé doit figurer sur la Demande d'attribution de titre abrégé pour ce titre abrégé. L'information contenue dans les cases A, C et D doit être complète.

5.5.3.3 Demande d'attribution et de génération de titre abrégé

Le STAR crée une Demande d'attribution/génération de titre abrégé en utilisant un même formulaire de commande, car il n'est pas nécessaire de demander l'attribution d'un nouveau titre abrégé avant de demander la génération de la clé. On doit remplir le formulaire au complet.

5.5.3.4 Demande de modification

L'ID autorisé (Auth ID) crée une demande de modification pour modifier les attributs de la clé, pour modifier les ID autorisés et pour fournir de l'information révisée sur la génération ou la distribution, pour un titre abrégé spécifique. L'information dans les cases A et D et tout changement requis dans les cases B et C doivent être complets.

5.5.3.5 Demande d'annulation

L'ID autorisé (Auth ID) crée une demande d'annulation pour annuler la production du titre abrégé d'une clé et pour dissocier les privilèges associés au titre abrégé de tous les ID EKMS. Les cases A et D doivent être remplies.

5.5.4 Titre abrégé

On doit entrer le titre abrégé pour les clés traditionnelles lors de demandes de génération, de modification et d'annulation. Le titre abrégé sera fourni par l'ICC sur le CRN de commande produit à la suite du traitement d'une Demande d'attribution du titre abrégé ou d'une Demande d'attribution/génération de titre abrégé.

5.5.5 Contrôle de la distribution

Le choix implicite ou explicite d'un contrôle de la distribution s'applique uniquement aux clés traditionnelles en format électronique. Le contrôle indique s'il existe ou non des restrictions au sujet de la distribution de ce titre abrégé de clé traditionnelle électronique. Si la clé est implicitement contrôlée, elle peut être distribuée conformément au profil de distribution pour le titre abrégé ou à la discrétion de l'autorité de contrôle pour le titre abrégé en cause. Quand la clé est explicitement contrôlée, le compte EKMS qui détient la clé doit avoir généré ou reçu des instructions de distribution électroniques avant la distribution de la clé.

5.5.6 Titre abrégé compatible

La sélection du titre abrégé compatible indique si la clé doit être livrée dans deux formats différents (c.-à-d. une clé sur support double). La clé sur support double est une clé identique présentée dans deux formats différents (p. ex., bande-clé sur papier et format électronique) et avec deux titres abrégés différents, que l'on peut utiliser sur un même réseau cryptographique. Les clés sur support double ne sont pas encore disponibles auprès de l'ICC.

5.5.7 ID autorisés

Cette case du formulaire de demande de clé permet à un OPM, un STAR ou un ID autorisé (Auth ID) d'attribuer la responsabilité de la commande de ce titre abrégé de clé. Les ID EKMS énumérés sont autorisés à présenter des demandes de génération, de modification et d'annulation, et de fournir des instructions de distribution pour ce titre abrégé.

5.5.8 Mécanisme de livraison

Si la clé doit être chargée directement dans un dispositif COMSEC comptable (p. ex., un DTD) par l'ICC pour sa livraison, le numéro de série du dispositif COMSEC (c.-à-d. équipement cryptographique) doit être inclus. Le formulaire de demande rempli et l'équipement cryptographique mis à zéro doivent être envoyés à l'ADN par l'intermédiaire du SNCMC.

5.5.9 Mise en garde CRYPTO

La mise en garde CRYPTO est utilisée pour indiquer la sensibilité unique de la clé. La clé est assujettie à des contrôles plus stricts régissant l'accès à celle-ci, sa distribution, son stockage, sa comptabilité, son utilisation, son élimination ou sa destruction. La mise en garde CRYPTO figurera en lettres grasses sur les couvertures du matériel de chiffrement imprimé et des codes, sur les disques et sur les variables de clés individuelles ou liées à titre d'attributs au titre abrégé de la clé électronique. Elle est appliquée au matériel de chiffement opérationnel, de diversification, de test et d'exercice (en sus de la classification ou de la désignation de sécurité). Les clés de maintenance et de formation en salle de classe ne portent habituellement pas la mise en garde CRYPTO.

5.5.10 Restrictions de traitement

Cette case indique toute restriction relative au traitement de la clé. La restriction « Remplissage bénin » indique que la clé peut être livrée uniquement dans l'équipement cryptographique à l'aide de techniques bénignes. La restriction « TPI » indique que l'intégrité de deux personnes est requise lors de la manipulation de la clé.

NOTE 1 : Si on sélectionne « TPI » pour la livraison des clés en format électronique, certaines opérations LMD/KP nécessiteront l'ouverture d'une session par un deuxième opérateur.

NOTE 2 : Les clés bénignes ne sont actuellement pas disponibles auprès de l'ICC.

5.5.11 Diffusion

Cette case sert à indiquer si la clé sera diffusée à l'extérieur du Canada et à qui sa diffusion est autorisée (c.-à-d. É.-U., OTAN).

5.5.12 Utilisation de la clé

L'utilisation prévue de la clé comprend :

a. FFK – Clé FIREFLY – utilisée pour établir une clé de chiffrement de clés (KEK) ou une clé de chiffrement du trafic (TEK) entre deux entités. La KEK ou TEK générée à partir d'un échange FIREFLY est ensuite utilisée dans un algorithme de chiffrement symétrique.
b. KEK – Clé de chiffrement de clés – utilisée pour chiffrer des clés.
c. KPK – Clé de production de clés – utilisée pour produire des clés.
d. NFK – Clé FIREFLY à réseau.
e. QKEK –Clé de chiffrement de clés quadrant.

f. TEK – Clé de chiffrement du trafic – utilisée pour chiffrer le trafic sur une voie de communication.

g. TSK – Clé TRANSEC– utilisée pour protéger une voie de communication contre l'analyse du trafic.

h. TrKEK – Clé de chiffrement de clé de transfert – utilisée par le KP et le DTD.

Les choix d'utilisation de clé ne sont pas tous disponibles pour chaque type d'équipement. Veuillez communiquer avec le CAGMC pour avoir de l'assistance afin de déterminer quelle utilisation convient à l'équipement auquel est destinée la clé.

5.5.13 But de la clé

Les choix de but de la clé ne sont pas tous disponibles pour chaque type d'équipement. Veuillez communiquer avec le CAGMC pour avoir de l'assistance afin de déterminer quel but convient à l'équipement auquel est destinée la clé.

5.5.14 Taille du réseau cryptographique

Quand on prévoit la mise en œuvre d'un réseau cryptographique, le chef des Services à la clientèle de la Sécurité cryptographique du CST doit être informé de la taille du réseau cryptographique et de l'autorité de contrôle proposée pour celui-ci. Les modifications importantes de la taille du réseau cryptographique doivent être signalées au CST, qui réévaluera la situation.

5.5.15 Cryptopériode

La cryptopériode est indiquée en heures, jours, semaines, mois ou années, et elle représente la durée pendant laquelle chaque clé est en vigueur. Il faut indiquer cette période.

5.5.16 Segment par édition

On doit inscrire le nombre de segments requis pour une même édition de la clé.

5.5.17 Fréquence de remplacement

On doit indiquer la fréquence de remplacement en heures, jours, semaines, mois ou années, pour chaque segment de la clé.

5.5.18 Date d'entrée en vigueur

Une fois remplie, la demande de clé doit être classifiée au niveau minimal CONFIDENTIEL si elle contient la date d'entrée en vigueur, et au niveau NON CLASSIFIÉ si elle ne la contient pas.

5.5.19 Date de mise en place

On doit indiquer la date à laquelle la clé doit être reçue par les comptes EKMS énumérés dans le profil de distribution. Cette date doit tenir compte du délai d'exécution requis pour traiter la demande de clé, générer la clé et la livrer. Le temps d'exécution pour la génération et la distribution des produits sur papier est passablement plus long que pour les clés électroniques.

5.5.20 Commande permanente

Des commandes permanentes sont établies quand une clé est demandée fréquemment et qu'un calendrier de réapprovisionnement est établi. On élimine ainsi le besoin de devoir présenter de nouvelles demandes après les demandes initiales, à moins qu'il n'y ait des modifications dans les attributs de la demande originale (p. ex., ajout d'un nouveau membre au réseau), auquel cas une demande de modification doit être présentée. S'il ne s'agit pas d'une commande permanente, la génération de la clé est prévue une seule fois. S'il s'agit d'une commande permanente, la génération de la clé sera automatiquement reprogrammée.

5.5.21 Information sur l'édition

On doit indiquer la première édition (p. ex., A, EB), la dernière édition et le nombre total d'éditions qui seront générées pour cette demande de clé.

5.5.22 Profil de distribution

Le profil de distribution indique quels comptes EKMS recevront une clé ou un groupe de clés, quelles éditions de la clé ils recevront et combien de copies pour chaque édition.

5.5.23 Code de comptabilité (CC) et règles de lancement de rapport de transfert (TRI)

Le code de comptabilité (CC) sert à indiquer les contrôles comptables minimaux pour les articles COMSEC visés par le SNCMC.

CC-1 : Comptabilité continue par numéro de comptabilité ou numéro de registre à un COR.

CC-2 : Comptabilité continue par quantité à un COR.

CC-4 : Accusé de réception initial requis et comptabilité en fonction des directives locales par la suite.

CC-6 : Clé électronique suivie par l'EKMS GC; comptabilité continue, avec ou sans numéro de comptabilité, dans un COR.

CC-7 : Clé électronique suivie par le EKMS GC, accusé de réception initial requis, pas de rapport subséquent; tenue automatisée des dossiers locaux (comptabilité en fonction des directives locales par la suite).

1) Le CC d'une ligne d'article TRI prendra par défaut la valeur CC 1 si le TRI n'est pas dans une transaction BET, sauf selon la définition (3) ci-dessous.
2) Le CC d'une ligne d'article TRI prendra par défaut la valeur CC 6 si le TRI n'est pas dans une transaction BET, sauf selon la définition (3) ci-dessous.
3) Le CC d'une ligne d'article TRI prendra par défaut la valeur CC 4 au lieu de CC 1, et CC 7 au lieu de CC 6 quand :
   i) But de la clé = M (maintenance)
   ii) But de la clé = T (formation)
   iii) But de la clé = Z (test en direct) et
   iv) Classification = non classifié.

Veuillez communiquer avec le CAGMC pour obtenir de l’assistance au sujet de la sélection des CC pour le matériel COMSEC comptable.

5.6 Avis de confirmation/rejet de la commande (CRN de commande)

Après le traitement de chaque demande de clé, l'ICC génère un CRN de commande pour le compte EKMS qui a présenté la demande. Cet avis confirme ou rejette la demande. Un exemple de CRN de commande figure à l'Annexe N.

NOTE : Les CRN pour les demandes de clés traditionnelles ne sont pas pris en charge par l'ICC pour le moment.

.

Page intentionnellement laissée en blanc

Glossaire

Agent de sécurité du ministère (ASM)	Personne chargée d'élaborer, de mettre en œuvre, de coordonner et de surveiller un programme de sécurité du ministère qui soit conforme à la PGS et aux normes qui s'y rattachent.
Appareil terminal sécurisé (STE)	Terminal de télécommunication approuvé par le gouvernement et conçu pour assurer des connexions voix et données sécurisées, avec fonction de téléconférence et d'autres fonctionnalités basées sur un modèle de communications en couches.
Article cryptographique contrôlé (CCI)	Équipement sûr de télécommunications ou de traitement de l'information, équipement cryptographique connexe ou dispositif auxiliaire, non classifié lorsqu'il n'est pas mis à la clé (ou lorsqu'il est mis à la clé au moyen d'une clé non classifiée), mais qui fait l'objet d'un contrôle par un système de comptabilité.
Attributs de clé	Caractéristiques attribuées à un titre abrégé de clé spécifique (p. ex., CC, but de la clé, utilisation de la clé, etc.).
Authentification	Mesure conçue pour assurer une protection contre les imitations ou les transmissions frauduleuses en établissant la validité d'une transmission, d'un message ou d'un auteur.
Autorité COMSEC du ministère (ACM)	Personne désignée par l'agent de sécurité du ministère (ASM) et chargée par l'ASM d'élaborer, de mettre en œuvre, de coordonner et de surveiller un programme COMSEC du ministère qui soit conforme à la PGS et aux normes qui s'y rattachent.
Autorité de contrôle	Responsable officiel désigné pour diriger l'exploitation d'un réseau cryptographique et pour gérer l'utilisation opérationnelle et le contrôle du matériel de chiffrement attribué au réseau cryptographique.
Autorité de gestion des clés (AGC)	Personne de niveau supérieur nommée par l'autorité COMSEC du ministère (ACM) pour coordonner et superviser la gestion de clés STU III, SDNS ou MSK au sein du ministère, de l'agence ou de l'organisme. **NOTE :** Aux États-Unis, l'autorité de gestion des clés est appelée *Command Authority*.

Autorité nationale de distribution (AND)	Entité nationale au sein du milieu COMSEC canadien chargée de recevoir, stocker, distribuer et éliminer en toute sécurité le matériel COMSEC provenant du CST ou reçu de pays étrangers ou encore destiné à ces pays.
Avis de confirmation/rejet (CRN)	Avis créé à la suite du traitement d'une Demande de clé ou d'une Demande d'établissement de privilèges (PER).
Bénin	Condition des données cryptographiques de sorte que celles-ci ne peuvent être compromises par un accès humain aux données.
Bigramme	Code à deux caractères qui indique le nombre de segments de clé dans une édition et la cryptopériode du segment de clé.
Bureau national des dossiers (NCOR)	Entité au sein de la section de contrôle COMSEC du CST chargée de tenir des registres permettant de rendre compte de tout le matériel COMSEC comptable produit au Canada ou confié à celui-ci.
Champ Classe 6	Champ qui figure sur l'afficheur à deux lignes du poste STU III distant. Le champ contient des données additionnelles de Classe 6 qui font partie du processus d'authentification. La ligne supérieure de l'afficheur indique le niveau de classification commun le plus élevé à la gauche et l'information sur le champ de code Classe 6 (p. ex., SCI) apparaît à la droite.
Chiffrement	Transformation des données en clair en chaînes de caractères inintelligibles au moyen d'un procédé réversible.
Clé	Information (habituellement sous forme d'une suite de nombres binaires aléatoires ou pseudo aléatoires), utilisée initialement pour configurer, puis par la suite modifier périodiquement les opérations effectuées par un équipement cryptographique afin de chiffrer ou de déchiffrer des signaux électroniques, de déterminer des mécanismes de contre-mesures électroniques (p. ex., saut de fréquence ou étalement de spectre), ou pour la production d'autres clés.
Clé alliée	Clé utilisée par au moins deux nations différentes. La clé alliée est générée par l'une des nations, puis communiquée aux autres nations pour être utilisée.

Clé de chiffrement de clé de transfert (TrKEK)	Clé utilisée pour chiffrer et déchiffrer des clés d'utilisateur.
Clé de chiffrement de clés (KEK)	Clé utilisée pour le chiffrement et le déchiffrement d'autres clés servant à la transmission ou au stockage.
Clé de chiffrement du trafic (TEK)	Clé servant à chiffrer du texte en clair, à surchiffrer un texte déjà chiffré ou à déchiffrer un texte chiffré.
Clé de diversification	Clé initiale contenant de l'information unique utilisée pour amorcer un processus de génération de clé ou de mise à jour.
Clé de production de clés (KPK)	Clé utilisée pour initialiser un générateur de flot de clés pour la production d'autres clés générées de manière électronique.
Clé de remplissage bénin	Matériel cryptographique FIREFLY de remplissage bénin utilisé par les processeurs de clés (KP) et l'équipement cryptographique de destination pour créer les clés servant à chiffrer/déchiffrer le matériel cryptographique d'application et les données d'utilisateur.
Clé de signature de message (MSK)	Matériel cryptographique, utilisé dans un processus de signature numérique, qui traite un message afin d'assurer l'authentification de la source du message, l'intégrité du message et la non-répudiation de la source.
Clé de test	Clé destinée aux tests en direct d'équipement ou de systèmes COMSEC.
Clé de type 0	Clé cryptographique utilisée pour générer une clé de chiffrement de clés (KEK) pouvant servir à chiffrer en vrac des clés.
Clé de type 1	Clé cryptographique utilisée pour protéger l'information classifiée jusqu'au niveau TRÈS SECRET, inclusivement.
Clé de type 2	Clé cryptographique utilisée pour protéger l'information désignée jusqu'au niveau PROTÉGÉ C, inclusivement.
Clé d'exercice	Clé destinée à protéger les transmissions associées à des exercices.

Clé étrangère	Clé nationale dont l'utilisation par une autre nation ou alliance a été autorisée. **NOTE :** C'est seulement dans des circonstances extrêmes qu'une clé nationale devrait être utilisée par une autre nation ou alliance.
Clé explicite	Toute clé qui fait l'objet d'un contrôle automatique par l'EKMS, conformément aux restrictions de distribution prescrites par l'autorité de contrôle.
Clé FIREFLY à réseau	Clé FIREFLY qui est gérée de la même façon qu'un réseau cryptographique traditionnel.
Clé implicite	Toute clé dont les caractéristiques de traitement sont déterminées uniquement par les politiques et les procédures appropriées.
Clé moderne	Nom collectif pour les clés articulées sur l'algorithme FIREFLY, telles les clés STU III, les clés de communications SDNS et les clés MSK.
Clé nationale	Clé utilisée uniquement par la nation qui l'a générée.
Clé opérationnelle	Clé destinée à une utilisation sur voie radio pour la protection des informations opérationnelles ou pour la production ou transmission électrique protégée de flots de clés.
Clé OTAN	Clé qui a été produite pour être utilisée par les pays de l'OTAN.
Clé SCI	Matériel de chiffrement STU III qui permet d'afficher l'authentificateur SCI dans le champ Classe 6 d'un poste distant, en mode sécurisé, si les deux terminaux contiennent le même désignateur.
Clé sur support double	Clé compatible qui existe à la fois en format électronique et en format physique.
Clé tactique	Clé de chiffrement du trafic, clé de chiffrement de clés ou clé de sécurité des transmissions conçue pour sécuriser l'information ou les données qui sont périssables, qui ont peu de valeur au point de vue renseignement (c.-à-d. faible sensibilité nationale ou internationale) et dont la classification n'est pas supérieure au niveau SECRET.
Clé traditionnelle	Terme utilisé pour faire référence à une clé non articulée sur l'algorythme FIREFLY qui est générée conformément à des procédures établies.

Code DAO	Identificateur unique de ministère, d'agence ou d'organisme utilisé dans les portions utilisateur d'une clé FIREFLY.
Code de Classe 6	Code à deux chiffres correspondant à un champ Classe 6 spécifique.
Code de comptabilité (CC)	Code numérique servant à indiquer les contrôles de comptabilité minimaux dont doivent faire l'objet les articles COMSEC enregistrés dans le Système national de contrôle du matériel COMSEC (SNCMC).
Command Authority	Voir Autorité de gestion des clés (AGC).
Compromission	Divulgation, destruction, suppression, modification ou interruption non autorisées.
Compte COMSEC	Entité administrative identifiée par un ID EKMS servant à la comptabilité, à la garde et au contrôle du matériel COMSEC comptable.
Compte EKMS	Terme générique qui désigne un élément EKMS ou un compte COMSEC.
Confidentialité	Sensibilité de l'information ou de biens à l'égard de leur divulgation non autorisée, cette sensibilité étant désignée par une classification ou une désignation, et chaque niveau de classification et de désignation correspondant à un degré de préjudice qui se produirait advenant la divulgation non autorisée.
CRYPTO	Mise en garde que l'on appose sur le matériel de chiffrement pour indiquer que chaque article ainsi marqué est soumis à des contrôles précis quant à son accès, à sa distribution, à son stockage, à sa comptabilisation, à son déclassement et à sa destruction.
Cryptopériode	Période de temps précise durant laquelle une clé de chiffrement est en vigueur.
Date d'entrée en vigueur	Date à laquelle une clé ou d'autres données sont censées être utilisées la première fois.
Déchiffrement	Processus qui convertit en clair les données ou la voix, en inversant le processus de chiffrement.
Demande d'établissement de privilèges (PER)	Transaction qui consiste à demander l'inscription, la modification ou la suppression de privilèges de commandes de clé (c.-à-d. OPM, STAR, représentant des utilisateurs) à un compte générateur.

Demandeur d'attribution de titre abrégé (STAR)	Compte EKMS autorisé à demander l'attribution de nouveaux titres abrégés à un compte générateur.
Destruction	Processus de destruction du matériel COMSEC physique (p. ex., par déchiquetage, incinération, etc.), ou destruction des clés électroniques par remise à zéro ou remplissage dans un équipement de destination.
Dispositif de gestion locale (LMD)	Composante dans l'EKMS qui assure des services automatisés pour la gestion des clés et autre matériel COMSEC, et constitue une interface permettant d'incorporer des fonctionnalités additionnelles, afin d'en accroître les capacités locales. Ce dispositif comprend la plate-forme fournie par l'utilisateur, le système d'exploitation et le logiciel EKMS.
Dispositif de remplissage	Article COMSEC utilisé pour transférer ou stocker une clé en format électronique, ou pour charger une clé dans un équipement cryptographique.
Dispositif de stockage de clés (KSD)	Dispositif de remplissage utilisé pour stocker, transporter et transférer des clés et d'autres données système.
Dispositif de transfert des données (DTD)	Dispositif de remplissage conçu pour stocker, transporter et transférer électroniquement et en toute sécurité à la fois des clés COMSEC et des clés TRANSEC. De conception rétrocompatible à la génération précédente de dispositifs de remplissage COMSEC, ce dispositif peut être programmé pour prendre en charge les systèmes modernes de mission.
Distribution de clé	Mouvement sécurisé et contrôlé d'une clé, de son point de génération ou de stockage à son point d'utilisation ou de redistribution.
Édition	Chaîne alphabétique ou numérique qui identifie l’émission d'une série ou une version spécifique de matériel COMSEC associée au même titre abrégé.
EKMS GC	Ensemble interopérable de systèmes automatisés, d'installations et de composantes qui offrent des services pour commander, générer, distribuer et gérer le matériel COMSEC canadien pour les activités de gestion des clés au sein du gouvernement du Canada.

Équipement COMSEC	Équipement conçu pour assurer la sécurité des communications en convertissant l'information sous une forme incompréhensible par un intercepteur non autorisé et, subséquemment, en retransformant cette information dans sa forme originale à l'intention des destinataires autorisés; désigne également l'équipement conçu expressément pour faciliter le processus de conversion, ou pour en constituer un élément essentiel.
Équipement cryptographique de type 1	Équipement cryptographique classifié ou CCI contenant un algorithme de chiffrement et/ou d'échange de clés, approuvé par le CST pour protéger de l'information classifiée et désignée.
Équipement cryptographique de type 2	Équipement, ensemble ou composant cryptographique non classifié contenant un algorithme de chiffrement et/ou d'échange de clés, approuvé par le CST pour protéger de l'information désignée.
Équipement cryptographique de type 3	Équipement cryptographique contenant un algorithme public ou privé de chiffrement et/ou d'échange de clés, approuvé par le CST pour protéger de l'information désignée.
Équipement cryptographique de type 4	Équipement cryptographique contenant un algorithme public ou privé de chiffrement et/ou d'échange de clés, qui n'a pas été approuvé par le CST pour protéger de l'information.
Gardien COMSEC	Personne désignée par l'autorité appropriée et qui est responsable de la réception, de la garde, de la distribution, de la protection, du transfert, de la comptabilité et de la destruction du matériel COMSEC porté à un compte COMSEC.
Génération	Processus selon lequel la première instance d'une clé est créée. Toutes les données dépendantes ou indépendantes du système de mission qui peuvent être tirées de la commande de clé sont mises dans le format requis pour être chargées dans l'équipement COMSEC de destination.
Gestion des clés	Procédures et mécanismes de génération, de distribution, de remplacement, de stockage, d'archivage et de destruction des clés qui commandent les processus de chiffrement ou d'authentification.

Gestionnaire des certificats de privilèges (PCM)	Compte EKMS autorisé à créer des certificats de privilèges KP pour un ensemble spécifique de comptes EKMS équipés de KP.
Gestionnaire des privilèges de commande (OPM)	Compte EKMS autorisé à nommer d'autres comptes en tant qu'OPM ou demandeur d'attribution de titre abrégé (STAR), ou de mettre fin à ces fonctions, à un compte générateur où il est inscrit en tant qu'OPM.
ID autorisé (Auth ID)	Compte EKMS qui est autorisé à commander un titre abrégé précis de clé traditionnelle.
ID EKMS	Identificateur unique de compte EKMS.
Identificateur d'affiliation nationale (NAI)	Code de pays à deux lettres, tiré du document ISO 3166 de l'Organisation internationale de normalisation, portant sur les codes qui représentent les pays et leurs subdivisions.
Incident COMSEC	Tout événement qui peut mettre en danger la sécurité de l'information classifiée ou désignée du gouvernement et qui est stockée, traitée, transmise ou reçue durant le processus de télécommunication.
Information classifiée	Toute information liée à l'intérêt national et qui pourrait faire l'objet d'une exception ou d'une exclusion en vertu de la *Loi sur l'accès à l'information* ou de la *Loi sur la protection des renseignements personnels*, mais dont la compromission, selon toute vraisemblance, porterait atteinte à l'intérêt national.
Inscription du compte	Processus par lequel les comptes EKMS GC sont identifiés et associés à leurs attributs administratifs et de configuration.
Installation centrale canadienne (ICC)	Entité au sein du CST qui fournit des services centralisés de gestion des clés pour toutes les sortes de clés.
Intégrité	Exactitude et intégralité de l'information et des biens, et authenticité des transactions.
Intégrité par deux personnes (TPI)	Procédure selon laquelle le matériel n'est jamais traité par une seule personne ou remis à une seule personne.

Matériel COMSEC	Matériel conçu pour protéger et authentifier les télécommunications. Le matériel COMSEC comprend, sans s'y limiter, les clés, l'équipement, les dispositifs, les documents, les microprogrammes et les logiciels qui comportent ou décrivent une logique cryptographique et d'autres articles qui exécutent des fonctions COMSEC.
Mise à la clé bénigne	Méthode de mise à la clé qui permet de générer et de chiffrer des clés dans les composantes de l'EKMS GC, comme le processeur de clés ou l'Installation centrale canadienne. Cette méthode permet également de livrer la clé à l'utilisateur sans que la clé ne doive être déchiffrée, et ce, jusqu'à ce qu'elle soit chargée dans l'équipement cryptographique de destination.
Mise à zéro	Suppression ou élimination de la clé d'un équipement cryptographique ou d'un dispositif de remplissage.
Non-répudiation	La non-répudiation permet de démontrer qu'une transaction a bel et bien eu lieu, ou encore que le message a été envoyé et reçu. Les parties en cause ne peuvent donc pas nier que l'échange a eu lieu.
Numéro d’identification de matériel de chiffrement (KMID)	Nombre qui identifie de manière unique une clé FIREFLY. Utilisé pour l'ajout ou pour le retrait d'un élément sur la liste des clés compromises (CKL) et pour comptabiliser les clés FIREFLY.
Numéro de registre	Numéro utilisé pour identifier de manière unique les copies individuelles de clés qui portent le même titre abrégé et la même édition. Synonyme de numéro de comptabilité.
Poste cryptophonique de troisième génération (STU III)	Terminal de télécommunication approuvé par le gouvernement et conçu pour protéger la transmission de l'information sensible ou classifiée en mode voix, données ou télécopieur.
Processeur de clés (KP)	Composante cryptographique de l'EKMS, conçue pour assurer la génération locale du matériel cryptographique, le chiffrement et le déchiffrement des clés, le chargement des clés dans les dispositifs de remplissage et des fonctions de signature et de vérification des messages.

Produits cryptographiques sur format physique	Clés, publications, listes de clés, etc., qui existent sous forme physique.
Profil de distribution	Liste fournie par le demandeur d'une clé ou une autorité de contrôle, décrivant en détail qui devrait recevoir une clé ou un groupe de clés et combien de copies de chaque clé ces personnes devraient recevoir.
Remise à la clé	Processus qui consiste à remplacer périodiquement tout le matériel de chiffrement FIREFLY, y compris les clés FIREFLY à remplissage bénin.
Remplacement	Remplacement prévu ou non prévu d'une clé ou d'une aide COMSEC par une édition différente.
Remplissage	Processus consistant à charger le matériel de chiffrement dans l'équipement cryptographique de destination pour son utilisation interne.
Renseignements cloisonnés de nature délicate (SCI)	Renseignements nécessitant des contrôles spéciaux et indiquant un accès restreint.
Représentant des utilisateurs	Personne officiellement désignée par l'autorité de gestion des clés (AGC) pour commander des clés STU III, SDNS ou MSK.
Réseau cryptographique	Ensemble d'équipements cryptographiques exploitant une même clé de chiffrement du trafic.
Réseau cryptographique gouvernemental (RCG)	Système informatisé qui prend en charge la gestion des clés pour les STU III en assurant la génération et la distribution des clés au Canada.
Restrictions de traitement	Moyen permettant de contrôler l'utilisation des clés traditionnelles. Les choix sont les suivants : pas de restriction, intégrité par deux personnes (TPI), remplissage bénin seulement.
Secure Data Network System (SDNS)	Système de mission qui est abonné aux services EKMS et qui assure la prestation de services de sécurité de bout-en-bout pour l'échange de données entre des systèmes de traitement automatisé des données sur des réseaux de communication publics n'offrant aucun service de sécurité.

Sécurité des télécommunications (COMSEC)	Protection résultant de l'application de mesures de sécurité cryptographique, de sécurité des transmissions et de sécurité de rayonnement aux télécommunications et à l'équipement de traitement de l'information ainsi que de l'application d'autres mesures pertinentes à l'information et au matériel COMSEC. La COMSEC comprend également les instructions requises pour réaliser cette protection. Ces mesures sont destinées à empêcher la compromission de l'information stockée, transmise ou traitée par un système des technologies de l'information. La COMSEC est également destinée à assurer l'authenticité des télécommunications.
Segment	Clé traditionnelle valide pour une cryptopériode.
Signature numérique	Transformation cryptographique des données qui, une fois ajoutée à une unité de données, fournit les services d'authentification de l'origine, d'intégrité des données et de non-répudiation du signataire.
Titre abrégé	Combinaison de lettres et de chiffres attribués à certains articles COMSEC pour en faciliter le traitement, la comptabilité et le contrôle.
Transaction chiffrée en vrac (BET)	Transaction EKMS contenant la ou les clés chiffrées, les attributs des clés chiffrés et les rapports comptables chiffrés (transfert ou remise).
TrKEK de DTD	Clé utilisée pour chiffrer une clé remise à un DTD par un KP. Elle est également chargée dans un DTD afin de lui permettre de déchiffrer la clé pour son chargement dans un équipement de destination.

Page intentionnellement laissée en blanc

Bibliographie/références

Les références suivantes ont été utilisées pour la préparation de cette publication :

a. *Doctrine canadienne en matière de cryptographie visant le dispositif de transfert de données AN/CYZ-10/10A* (CCD-01), mai 1998, Centre de la sécurité des télécommunications.

b. *Doctrine canadienne en matière de cryptographie visant le Système canadien de chiffrement réseau* (CCD-02), septembre 1998, Centre de la sécurité des télécommunications.

c. *Doctrine canadienne en matière de cryptographie visant le CipherTAC 2000* (CCD-04), janvier 1999, Centre de la sécurité des télécommunications.

d. *Doctrine canadienne en matière de cryptographie visant l'unité canadienne de gestion des clés (CKMU)* (CCD-05), avril 2000, Centre de la sécurité des télécommunications.

e. *Doctrine canadienne en matière de cryptographie visant le Système de gestion électronique des clés du gouvernement du Canada (EKMS GC)* (CCD-06), ébauche juin 2000, Centre de la sécurité des télécommunications.

f. *Lignes directrices en matière de sécurité des télécommunications* (ITSD-01), ébauche mai 2001, Centre de la sécurité des télécommunications.

g. *Nomenclature des titres abrégés au Canada* (ITSG-09), octobre 2001, Centre de la sécurité des télécommunications.

h. *Doctrine canadienne en matière de cryptographie visant la carte cryptographique FORTEZZA PLUS (KOV- 14C) et l'appareil téléphonique sûr (STE)* (CCD-11), avril 2002, Centre de la sécurité des télécommunications.

i. *Manuel de contrôle du matériel COMSEC* (ITSG-10) (anciennement MG-14), janvier 2003, Centre de la sécurité des télécommunications.

j. *Doctrine canadienne en matière de cryptographie visant le dispositif de gestion locale/ processeur de clés (LMD/KP)* (CCD-07), août 2002, Centre de la sécurité des télécommunications.

Page intentionnellement laissée en blanc

Annexe A – Points de contact au CST

A.1 Généralités

Cette annexe contient les numéros de téléphone ainsi que les adresses électroniques et postales des points de contact au CST.

A.2 Centre d'assistance et de gestion du matériel cryptographique (CAGMC)

Numéro de téléphone : (613) 991-8600

Adresse électronique : CMAC@cse-cst.gc.ca

Télécopieur non classifié : (613) 991- 7440

Télécopieur sécurisé : (613) 991-8709

A.3 Bureau national des incidents COMSEC (BNIC)

Numéro de téléphone : (613) 991-8498

Adresse électronique : ncio@cse-cst.gc.ca

Télécopieur non classifié : (613) 991-8565

Télécopieur sécurisé : (613) 991-8565 (appelez le 991-8132 pour la configuration)

A.4 Bureau des procédures nationales en cryptographie, des vérifications et de la formation (PNCVF)

Numéro de téléphone : (613) 991-8173

Adresse électronique : ncpat@cse-cst.gc.ca

A.5 Chef, Services à la clientèle, Sécurité cryptographique

Numéro de téléphone : (613) 991-8495

Adresse électronique : its.client.services@cse-cst.gc.ca

Télécopieur non classifié : (613) 991-8565

Télécopieur sécurisé : (613) 991-8565 (appelez le 991-8132 pour la configuration)

A.6 Demandes de renseignements généraux au CST

Numéro de téléphone : (613) 991-7600

Site Web : http://www.cse-cst.gc.ca

Télécopieur non classifié : (613) 991-8565

Télécopieur sécurisé : (613) 991-8565 (appelez le 991-8132 pour la configuration)

Adresse postale du CST :

Centre de la sécurité des télécommunications
B.P. 9703
Terminus d'Ottawa
Ottawa (Ontario), Canada
K1G 3Z4

Aux soins de : _____

Nom Immeuble Poste

Adresse d'expédition du CST :

Centre de la sécurité des télécommunications
719, chemin Heron
Ottawa (Ontario), Canada
K1G 3Z4

Aux soins de : _____

Nom Immeuble Poste

Annexe B – Directive sur le contrôle des clés STU III pour les applications SCI

B.1 Objet

Cette directive établit des procédures et attribue des responsabilités pour l'acquisition et le contrôle des clés STU III pour les applications SCI (*renseignements cloisonnés de nature délicate*). Cette directive vise à assurer la mise en œuvre de procédures uniformes dans l'ensemble de la communauté des utilisateurs STU III au sein du gouvernement du Canada (GC).

B.2 Champ d'application

Cette directive s'applique à tous les ministères du GC qui participent au Réseau cryptographique gouvernemental (RCG) basé sur les téléphones STU III, de concert avec l'acquisition et le déploiement de terminaux STU III de type 1, dans les zones autorisées à traiter l'information SCI.

B.3 Définitions

Agent de sécurité du ministère (ASM)	Personne chargée d'élaborer, de mettre en œuvre, de tenir, de coordonner et de surveiller un programme de sécurité du ministère qui soit conforme à la PGS et aux normes qui s'y rattachent.
Autorité de gestion des clés (AGC)	Personne de niveau supérieur nommée par un ministère, une agence ou un organisme pour coordonner et superviser la gestion de clés STU III, SDNS ou MSK au sein du ministère, de l'agence ou de l'organisme.
Champ Classe 6	Champ qui figure sur l'afficheur à deux lignes du poste STU III distant. Le champ contient des données de Classe 6 additionnelles qui font partie du processus d'authentification. La ligne supérieure de l'afficheur indique le niveau de classification commun le plus élevé à la gauche et l'information sur le champ de code Classe 6 (p. ex., SCI) à la droite.
Clé SCI	Matériel de chiffrement STU III qui permet d'afficher l'authentificateur SCI dans le champ Classe 6 d'un poste distant, en mode sécurisé, si les deux terminaux contiennent le même désignateur.
Code de Classe 6	Code à deux chiffres correspondant à un champ Classe 6 spécifique.
Renseignements cloisonnés de nature délicate (SCI)	Renseignements nécessitant des contrôles spéciaux indiquant un accès restreint.
Représentant des utilisateurs (RU)	Personne officiellement nommée par une autorité de gestion des clés (AGC) pour commander des clés STU III, SDNS ou MSK.

B.4 Procédures et responsabilités des ministères

L'autorité de gestion des clés (AGC) établira les besoins du ministère pour ce qui est des clés SCI et désignera un ou plusieurs représentants des utilisateurs dans le ministère, par l'intermédiaire du processus d'inscription des représentants des utilisateurs. Le représentant des utilisateurs se verra attribuer l'autorité de commander des clés SCI de l'Installation centrale

canadienne (ICC), au CST, de la manière indiquée sur le formulaire Demande d'établissement de privilèges pour les clés STU III (PER pour clés STU III), à l'Annexe D. Le code DAO et la description DAO spécifiés pour la clé SCI devront comporter le mot CANADA sur la ligne 1.

Le représentant des utilisateurs indiquera les besoins du ministère en matière de clés SCI, en consultant l'agent de sécurité du ministère (ASM).

L'ASM vérifiera les points suivants :

a. l'habilitation de sécurité et le niveau d'endoctrinement des utilisateurs prévus des clés SCI;
b. la zone dans laquelle le poste STU III est situé a été autorisée à traiter l'information SCI;
c. de plus, il authentifiera les commandes de clé SCI (anciennement RCD) pour STU III, en utilisant le formulaire Attestation – Demande de clés RCD (Annexe O).

Le représentant des utilisateurs préparera et présentera le formulaire Demande de clé STU III (Annexe J) pour les clés SCI au Centre d'assistance et de gestion du matériel cryptographique (CAGMC) du CST et avisera le gardien COMSEC de cette action. Le représentant des utilisateurs présentera également le formulaire Attestation – Demande de clé RCD au CAGMC.

Le gardien COMSEC fournira aux utilisateurs autorisés à utiliser des clés SCI les procédures de chargement, d'utilisation et de protection de la clé SCI.

B.5 Procédures et responsabilités de l'ICC

Le CAGMC vérifiera toutes les Demande de clés STU III pour la clé SCI, afin de s'assurer qu'elles correspondent aux privilèges attribués au représentant des utilisateurs par l'AGC, et il vérifiera la cosignature des ASM. En outre, le CAGMC s'assurera que le ministère a un compte COMSEC TRÈS SECRET inscrit auprès du Bureau national des dossiers (NCOR), tel qu'exigé pour la réception d'une clé SCI de niveau TRÈS SECRET.

Le CAGMC enverra le formulaire Demande de clé STU III pour la clé SCI à l'autorité du CST responsable de l'accréditation initiale et de la supervision de sécurité permanente, de concert avec l'ASM, des installations dans lesquelles l'information SCI est traitée. L'autorité du CST accordera l'autorisation finale pour ce qui est de la Demande de clé SCI.

Le CAGMC débutera le traitement de la Demande de clé STU III demandant une clé SCI et acheminera au représentant des utilisateurs un Avis de confirmation/rejet de commande de clé STU III.

Les procédures et installations de sécurité du ministère doivent être inspectées et approuvées avant la réception de la clé SCI. Le CST peut effectuer cette fonction ou en déléguer des éléments autorisés au sein du ministère demandeur.

B.6 Entrepreneurs

Le GC n'a pas besoin de remettre des clés SCI à des entrepreneurs, à l'heure actuelle.

Annexe C – Certificat de nomination

Communications Security Establishment / Centre de la sécurité des télécommunications

PROTECTED A (when completed)
PROTÉGÉ A (une fois rempli)

APPOINTMENT CERTIFICATE
CERTIFICAT DE NOMINATION

A. ACCOUNT INFORMATION/INFORMATION SUR LE COMPTE

1. EKMS ACCOUNT NAME/NOM DU COMPTE EKMS

2. EKMS ID/ID EKMS ☐☐☐☐☐☐

3. REQUEST TYPE / TYPE DE DEMANDE ☐ NEW APPOINTMENT / NOUVELLE NOMINATION ☐ TERMINATION OF APPOINTMENT / CESSATION DES FONCTIONS

B. ROLES/RÔLES

4. _____ HAS BEEN APPOINTED/TERMINATED AS: / ASSUME LES FONCTIONS/EST LIBÉRÉ DES FONCTIONS SUIVANTES :

- ☐ DEPARTMENTAL COMSEC AUTHORITY (DCA)/AUTORITÉ COMSEC DU MINISTÈRE (ACM)
- ☐ COMSEC CUSTODIAN/GARDIEN COMSEC
- ☐ ALTERNATE COMSEC CUSTODIAN/GARDIEN COMSEC SUPPLÉANT
- ☐ MSK -KEY MANAGEMENT AUTHORITY (KMA)/AUTORITÉ DE GESTION DES CLÉS (AGC)
- ☐ -USER REPRESENTATIVE/REPRÉSENTANT DES UTILISATEURS
- ☐ -ALTERNATE USER REPRESENTATIVE/REPRÉSENTANT DES UTILISATEURS SUPPLÉANT
- ☐ STU -KEY MANAGEMENT AUTHORITY (KMA)/AUTORITÉ DE GESTION DES CLÉS (AGC)
- ☐ -USER REPRESENTATIVE/REPRÉSENTANT DES UTILISATEURS
- ☐ -ALTERNATE USER REPRESENTATIVE/REPRÉSENTANT DES UTILISATEURS SUPPLÉANT
- ☐ SDNS -KEY MANAGEMENT AUTHORITY (KMA)/AUTORITÉ DE GESTION DES CLÉS (AGC)
- ☐ -USER REPRESENTATIVE/REPRÉSENTANT DES UTILISATEURS
- ☐ -ALTERNATE USER REPRESENTATIVE/REPRÉSENTANT DES UTILISATEURS SUPPLÉANT
- ☐ ORDERING PRIVILEGE MANAGER (OPM)/GESTIONNAIRE DES PRIVILÈGES DE COMMANDE (OPM)
- ☐ SHORT TITLE ASSIGNMENT REQUESTER (STAR)/DEMANDEUR D'ATTRIBUTION DE TITRE ABRÉGÉ (STAR)

SPECIMEN SIGNATURE / SPÉCIMEN DE LA SIGNATURE		EFFECTIVE DATE (YYYY/MM/DD) / DATE D'ENTRÉE EN VIGUEUR (AAAA/MM/JJ)
TELEPHONE / TÉLÉPHONE	FAX	E-MAIL / COURRIEL

C. AUTHORIZATION OF APPOINTMENT/AUTORISATION DE LA NOMINATION

5. I HAVE CONFIRMED THAT THE APPOINTEE MEETS ALL OF THE FOLLOWING REQUIREMENTS: / JE CONFIRME QUE LA PERSONNE NOMMÉE RÉPOND AUX CRITÈRES SUIVANTS :
   - A. IS A CANADIAN CITIZEN; / EST CITOYEN CANADIEN;
   - B. HAS BEEN GRANTED A SECURITY CLEARANCE AS INDICATED IN BOX 6; / A OBTENU UNE HABILITATION DE SÉCURITÉ AU NIVEAU INDIQUÉ DANS LA CASE 6;
   - C. HAS RECEIVED A COMSEC BRIEFING (IF APPLICABLE); / A ASSISTÉ À UNE SÉANCE D'INITIATION COMSEC (LE CAS ÉCHÉANT);
   - D. IS FULLY CONVERSANT WITH THE DUTIES AND RESPONSIBILITIES OF THE APPOINTMENT. / A PRIS CONNAISSANCE DE TOUTES LES TÂCHES ET RESPONSABILITÉS LIÉES AU POSTE.

NAME OF AUTHORITY/NOM DE L'AUTORITÉ _____ SIGNATURE _____ DATE _____

6. SECURITY CLEARANCE / HABILITATION DE SÉCURITÉ
   - ☐ TOP SECRET/TRÈS SECRET
   - ☐ SECRET
   - ☐ CONFIDENTIAL/CONFIDENTIEL
   - ☐ ENHANCED RELIABILITY CHECK / VÉRIFICATION APPROFONDIE DE LA FIABILITÉ
   - ☐ BASIC RELIABILITY CHECK / VÉRIFICATION DE BASE DE LA FIABILITÉ

DATE GRANTED (YYYY/MM/DD)/DATE D'OCTROI (AAAA/MM/JJ) _____

D. TERMINATION OF APPOINTMENT/CESSATION DES FONCTIONS

7. THE TERMINATION OF THE ABOVE NAMED INDIVIDUAL WILL BECOME EFFECTIVE ON THE DATE INDICATED IN BLOCK 4. / LA PERSONNE IDENTIFIÉE CI-DESSUS CESSERA SES FONCTIONS À PARTIR DE LA DATE INDIQUÉE DANS LA CASE 4.

NAME OF AUTHORITY/NOM DE L'AUTORITÉ _____ SIGNATURE _____ DATE _____

E. ACKNOWLEDGEMENT /ACCUSÉ DE RÉCEPTION

8. THIS IS TO ACKNOWLEDGE THAT THE CMAC HAS PROCESSED THIS REQUEST. / LE CAGMC ACCUSE RÉCEPTION DE CETTE DEMANDE ET CONFIRME QU'ELLE A ÉTÉ TRAITÉE.

NAME OF AUTHORITY/NOM DE L'AUTORITÉ _____ SIGNATURE _____ DATE _____

SEND COMPLETED FORMS TO:	VEUILLEZ ENVOYER LE FORMULAIRE AU :
COMMUNICATIONS SECURITY ESTABLISHMENT P.O. BOX 9703, TERMINAL OTTAWA ON K1G 3Z4 ATTN: CRYPTOMATERIAL MANAGEMENT AND ASSISTANCE CENTRE (CMAC)	CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS C.P. 9703, TERMINUS POSTAL OTTAWA (ONTARIO) K1G 3Z4 ATTENTION : CENTRE D'ASSISTANCE ET DE GESTION DU MATÉRIEL CRYPTOGRAPHIQUE (CAGMC)
IF YOU REQUIRE ASSISTANCE OR HAVE ANY QUESTIONS, PLEASE CONTACT CRYPTOMATERIAL MANAGEMENT AND ASSISTANCE CENTRE (CMAC) AT TEL (613) 991-8600, FAX (613) 991-7440 OR E-MAIL AT CMAC@CSE-CST.GC.CA	SI VOUS AVEZ BESOIN D'AIDE OU SI VOUS AVEZ DES QUESTIONS, VEUILLEZ COMMUNIQUER AVEC LE CENTRE D'ASSISTANCE ET DE GESTION DU MATÉRIEL CRYPTOGRAPHIQUE (CAGMC) PAR TÉLÉPHONE AU (613) 991-8600, PAR FAX AU (613) 991-7440 OU PAR COURRIEL À L'ADRESSE CMAC@CSE-CST.GC.CA.

RESET

CSE 675 (04-04)

INSTRUCTIONS

GENERAL

Appointee must be a Canadian citizen, who, if requires access to material, possesses a security clearance or reliability status at least equal to the highest security classification or protection of the material held in the account. The Departmental COMSEC Authority (DCA) or the Departmental Security Officer (DSO) must carefully screen personnel, in order to ensure that each individual selected is a responsible individual, who is qualified to assume the duties and responsibilities associated with the position. Selected individuals must have enough autonomy to exercise proper jurisdiction in fulfilling his/her responsibilities; can perform their COMSEC functions on an as required basis; can serve for at least one year in order to reduce the possibility of frequent replacement; and, has not been relieved previously of COMSEC duties for reasons of negligence or non-performance of duties.

Section A - Account Information

Block 1. **EKMS Account Name:** Enter the exact name that appears on all accounting reports and associated correspondence. Write name in full, no abbreviations.

Block 2. **EKMS ID:** Enter the full 6 digit EKMS ID corresponding to Number 1.

Block 3. **Request Type (Select one):** Please select the appropriate action. If you're appointing a new member please carefully read above instructions.

Section B - Roles

Block 4. Print name of individual being appointed to, or terminated from this EKMS account. Write name in full, e.g. John Robert Smith vice J.R. Smith. **One form per individual**. The role of the DCA and COMSEC Custodian **shall not** be performed by the same individual. The account requires at a minimum a DCA or a DSO; a COMSEC Custodian and an Alternate COMSEC Custodian (may be assigned multiple roles). **For appointments provide Specimen Signature**.

Section C - Authorization of Appointment

Block 5. **Authorization** - The DSO or the DCA shall approve the official appointment. Appointee must meet all listed pre-requisites and must be either fully conversant with the duties and responsibilities associated with the appointment or will soon be attending all requisite training as provided by the CSE ITS Learning Centre (ITSLC).

Block 6. **Security Clearance** - Provide highest level and enter date granted.

Section D - Termination of Appointment

Block 7. **Name of Authority** - Either the DCA or the DSO is authorized to approve the Termination of Appointment. Please include the effective date and send completed forms to the CMAC. Do not forget to re-appoint another individual if required.

Section E - Acknowledgement

(For CMAC use only)

DIRECTIVES

GÉNÉRALITÉS

La personne nommée doit être un citoyen canadien qui, s'il doit accéder au matériel, bénéficie d'une cote de sécurité ou de fiabilité égale ou supérieure à la classification ou désignation la plus élevée du matériel détenu au compte. L'autorité COMSEC du ministère (ACM) ou l'agent de sécurité du ministère (ASM) doit sélectionner le personnel avec soin afin de s'assurer que chaque personne est qualifiée pour assumer les devoirs et responsabilités associés à son poste. Chaque personne sélectionnée doit avoir un degré d'autonomie suffisant pour exercer les pouvoirs appropriés à l'exécution de ses obligations; peut exercer ses fonctions COMSEC selon les besoins; peut demeurer en fonction pendant au moins un an afin de réduire la possibilité de remplacements fréquents; ne doit pas avoir été libérée précédemment de ses fonctions COMSEC pour négligence ou manquement au devoir.

Section A – Information sur le compte

Case 1. **Nom du compte :** Entrez le nom exact qui apparaît dans tous les rapports comptables et sur toute correspondance connexe. Inscrivez le nom au complet, sans abréviations.

Case 2. **ID EKMS :** Entrez l'ID EKMS de six chiffres associé au compte de la case 1.

Case 3. **Type de demande** (en choisir une) : Choisissez l'option appropriée. Si vous nommez un nouveau membre, lisez attentivement les directives ci-dessus.

Section B – Rôles

Case 4. Inscrivez le nom de personne qui entre en fonction ou qui quitte ses fonctions au compte EKMS. Écrivez le nom au long, p. ex. Paul Pierre Durant au lieu de P. P. Durant. **Il faut remplir une demande par personne**. La même personne **ne peut pas** être à la fois ACM et gardien COMSEC. Le compte doit avoir au moins un ACM ou un ASM, un gardien COMSEC et un gardien COMSEC suppléant (qui peut être nommé à plusieurs rôles). **En cas de nomination, il faut fournir un spécimen de la signature**.

Section C – Autorisation de la nomination

Case 5. **Autorisation** – L'ASM ou l'ACM doit approuver la nomination officielle. La personne nommée doit répondre à tous les critères énumérés et doit soit connaître toutes les tâches et responsabilités liées au poste soit bientôt assister à la formation obligatoire offerte par le Centre de formation en STI du CST (CFSTI).

Case 6. **Habilitation de sécurité** – Indiquez le niveau le plus élevé et la date à laquelle l'habilitation a été accordée.

Section D – Cessation des fonctions

Case 7. **Nom de l'autorité** – Seul l'ASM ou l'ACM peut approuver la cessation des fonctions. Indiquez la date d'entrée en vigueur et envoyez le formulaire rempli au CAGMC. N'oubliez pas de nommer une nouvelle personne, au besoin.

Section E – Accusé de réception

(À l'usage du CAGMC)

CSE 675 (04-04)

Annexe D – Demande d'établissement de privilèges (PER) pour clés STU III

Communications Security Establishment / Centre de la sécurité des télécommunications

PROTECTED A (when completed)
PROTÉGÉ A (une fois rempli)

STU-III PRIVILEGE ESTABLISHMENT REQUEST (PER)
DEMANDE D'ÉTABLISSEMENT DE PRIVILÈGES (PER) POUR CLÉS STU-III

A. ACCOUNT INFORMATION/INFORMATION SUR LE COMPTE

1. FROM/DE — EKMS ID/ID EKMS ☐☐☐☐☐☐
NAME/NOM
NO./N° STREET/RUE
CITY/VILLE PROVINCE POSTAL CODE/CODE POSTAL

2. TRANSACTION ID/ID DE LA TRANSACTION
☐☐☐☐☐☐ ☐☐☐☐/☐☐/☐☐ ☐☐☐☐
EKMS ID/ID EKMS DATE (YYYY/MM/DD-AAAA/MM/JJ)

B. USER REPRESENTATIVE - STU-III KEY ORDERING PRIVILEGES
REPRÉSENTANT DE L'UTILISATEUR - PRIVILÈGES DE COMMANDE DE CLÉ STU-III

3. REQUEST TYPE / TYPE DE DEMANDE ☐ ADD / AJOUT ☐ MODIFY / MODIF. ☐ DELETE / SUPPR. DAO CODE/CODE DAO	4. DAO DESCRIPTION/ DESCRIPTION DAO LINE 1/LIGNE 1 LINE 2/LIGNE 2
5. REQUEST TYPE / TYPE DE DEMANDE ☐ ADD / AJOUT ☐ MODIFY / MODIF. ☐ DELETE / SUPPR. DAO CODE/CODE DAO	6. DAO DESCRIPTION/DESCRIPTION DAO LINE 1/LIGNE 1 LINE 2/LIGNE 2
7. REQUEST TYPE / TYPE DE DEMANDE ☐ ADD / AJOUT ☐ MODIFY / MODIF. ☐ DELETE / SUPPR. DAO CODE/CODE DAO	8. DAO DESCRIPTION/DESCRIPTION DAO LINE 1/LIGNE 1 LINE 2/LIGNE 2
9. REQUEST TYPE / TYPE DE DEMANDE ☐ ADD / AJOUT ☐ MODIFY / MODIF. ☐ DELETE / SUPPR. DAO CODE/CODE DAO	10. DAO DESCRIPTION/DESCRIPTION DAO LINE 1/LIGNE 1 LINE 2/LIGNE 2
11. EKMS ACCOUNT NAME / NOM DU COMPTE EKMS PRIVILEGE FOR EKMS ID / PRIVILÈGE POUR L'ID EKMS	12. EKMS USE INDICATOR / INDICATEUR D'UTILISATION EKMS ☐ YES / OUI ☐ NO / NON

13. AUTHORIZED KEY TYPE / TYPE DE CLÉ AUTORISÉE	TYPE 1	TYPE 2
CANADIAN SEED / CANADIENNE, DIVERSIFICATION	☐	☐
CANADIAN OPERATIONAL / CANADIENNE, OPÉRATIONNELLE	☐	☐
U.S SEED / AMÉRICAINE, DIVERSIFICATION	☐	☐
U.S. OPERATIONAL / AMÉRICAINE, OPÉRATIONNELLE	☐	☐

14. MAXIMUM KEY CLASSIFICATION / CLASSIFICATION MAXIMALE DE LA CLÉ
☐ TOP SECRET / TRÈS SECRET
☐ SECRET
☐ CONFIDENTIAL / CONFIDENTIEL
☐ UNCLASSIFIED / NON CLASSIFIÉ

15. CLASS 6 CODE (Optional) / CODE DE CLASSE 6 (facultatif)
☐ 01 – PROTECTED C / 01 – PROTÉGÉ C
☐ 02 – PROTECTED B / 02 – PROTÉGÉ B
☐ 03 – PROTECTED A / 03 – PROTÉGÉ A
☐ 10 - SCI
☐ 20 – U.S.
☐ 25 - MOBILE

C. STU-III KMA APPROVAL
APPROBATION DE L'AGC STU-III

I HEREBY CERTIFY THAT THE STU-III USER REPRESENTATIVE AND ALTERNATE USER REPRESENTATIVES REGISTERED WITH THIS EKMS ACCOUNT ARE AUTHORIZED TO ORDER STU-III KEY WITH THE PRIVILEGES INDICATED HEREIN. THE STU-III KMA SIGNING THIS FORM MUST BE REGISTERED WITH THIS EKMS ACCOUNT.
JE, SOUS-SIGNÉ, CERTIFIE QUE LE REPRÉSENTANT DE L'UTILISATEUR ET LES REPRÉSENTANTS SUPPLÉANTS DE L'UTILISATEUR STU-III INSCRITS À CE COMPTE SONT AUTORISÉS À COMMANDER UNE CLÉ STU-III EN VERTU DES PRIVILÈGES INDIQUÉS DANS LA PRÉSENTE. L'AGC STU-III QUI SIGNE LE FORMULAIRE DOIT ÊTRE INSCRIT À CE COMPTE EKMS.

NAME/NOM | SIGNATURE | DATE

D. SUBMIT FORMS/ENVOI DES FORMULAIRES

SEND COMPLETED FORMS TO:
COMMUNICATIONS SECURITY ESTABLISHMENT
P.O. BOX 9703, TERMINAL
OTTAWA ON K1G 3Z4
ATTN: CRYPTOMATERIAL MANAGEMENT AND ASSISTANCE CENTRE (CMAC)

VEUILLEZ ENVOYER LE FORMULAIRE AU :
CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS
C.P. 9703, TERMINUS POSTAL
OTTAWA (ONTARIO) K1G 3Z4
ATTENTION : CENTRE D'ASSISTANCE ET DE GESTION DU MATÉRIEL CRYPTOGRAPHIQUE (CAGMC)

IF YOU REQUIRE ASSISTANCE OR HAVE ANY QUESTIONS, PLEASE CONTACT CRYPTOMATERIAL MANAGEMENT AND ASSISTANCE CENTRE (CMAC) AT TEL (613) 991-8600, FAX (613) 991-7440 OR E-MAIL AT CMAC@CSE-CST.GC.CA

SI VOUS AVEZ BESOIN D'AIDE OU SI VOUS AVEZ DES QUESTIONS, VEUILLEZ COMMUNIQUER AVEC LE CENTRE D'ASSISTANCE ET DE GESTION DU MATÉRIEL CRYPTOGRAPHIQUE (CAGMC) PAR TÉLÉPHONE AU (613) 991-8600, PAR FAX AU (613) 991-7440 OU PAR COURRIEL À L'ADRESSE CMAC@CSE-CST.GC.CA.

RESET

CSE 673 (02-04)

INSTRUCTIONS

Section A

Block 1. Enter the name of the EKMS ID submitting the PER.

Block 2. Enter the Transaction ID for the PER. It includes the EKMS Id of the STU-III Key Management Authority (KMA) that is submitting the PER, the current date in YYYYMMDD format, and a one up sequence number for the current calendar year.

Section B

Block 3-5-7-9. - Select "Add" to add one STU-III privilege. The CMAC will assign the DAO code.
- Select "Modify" to modify an existing STU-III privilege. Provide the DAO code that will be replaced.
- Select "Delete" to delete all STU-III ordering privileges associated with the specified DAO code. Provide the DAO code that will be deleted.

Block 4-6-8-10. Enter the DAO description that will be or is associated with the DAO code (for block 4 see block 3, for 6 see 5, for 8 see 7 and for 10 see 9). The DAO description consists of either one or two lines of information. Each line may contain up to 16 characters including spaces.

Block 11. Enter the EKMS ID and name receiving the privilege.

Block 12. Select yes if the key is to be use for the LMD/KP.

Block 13. Select the type(s) of key that may be ordered.

Block 14. Select one classification. Must not be higher than the privileged EKMS ID's Highest Classification Indicator (HDI) or clearance.

Block 15. Optional. Select one or more Class 6 code.
- 01 if requesting PROTECTED C ordering privileges.
- 02 if requesting PROTECTED B ordering privileges.
- 03 if requesting PROTECTED A ordering privileges.
- 10 if requesting Sensitive Compartmented Information (SCI) ordering privileges. This code is associated with TOP SECRET key only.
- 20 if requesting U.S. key ordering privileges.
- 25 if requesting CipherTAC 2000 ordering privileges.

Section C

The STU-III KMA of the EKMS ID submitting the PER must print and sign his or her name and enter the current date on the form.

DIRECTIVES

Section A

Case 1. Entrez le nom du compte EKMS qui fait la demande.

Case 2. Entrez l'ID de la transaction de la demande, notamment l'ID EKMS de l'autorité de gestion des clés (AGC) STU-III qui présente la demande, la date en format AAAAMMJJ et un numéro ascendant selon l'année civile en cours.

Section B

Case 3-5-7-9. - Choisissez "Ajout" pour ajouter un privilège STU-III. Le CAGMC attribura le code DAO.
- Choisissez "Modifier" pour modifier un privilège STU-III existant. Veuillez indiquer le code DAO à modifier.
- Choisissez "Supression" pour supprimer tout privilège de commande STU-III associé au code DAO spécifié. Veuillez indiquer le code DAO à supprimer.

Case 4-6-8-10. Entrez la description DAO qui sera ou est associée au code DAO (pour la case 4 voir la case 3, pour la case 6 voir la case 5, pour la case 8 voir la case 7 et pour la case 10 voir la case 9). La description DAO se compose d'une ou de deux lignes d'information. Chaque ligne peut contenir un maximum de 16 caractères.

Case 11. Entrez le nom et l'ID EKMS du compte qui reçoit le privilège.

Case 12. Si la clé doit être utilisée pour le LMD/KP, cochez la case Oui.

Case 13. Choisissez le ou les types de clé qui pourront être commandés.

Case 14. Choisissez une classification. Celle-ci ne doit pas être supérieure à l'indicateur de classification de plus élevé (HCI) ou à l'habilitation de l'ID EKMS autorisé.

Case 15. Facultative. Choisissez un ou plusieurs codes de classe 6.
- 01 si vous demandez des privilèges de commande au niveau PROTÉGÉ C.
- 02 si vous demandez des privilèges de commande au niveau PROTÉGÉ B.
- 03 si vous demandez des privilèges de commande au niveau PROTÉGÉ A.
- 10 si vous demandez des privilèges de commande au niveau SCI (Renseignements compartimentés de nature délicate). Ce code ne peut être associé qu'avec une clé TRÈS SECRET.
- 20 si vous demandez des privilèges de commande pour clé américaine.
- 25 si vous demandez des privilèges de commande pour le CiperTAC 2000.

Section C

L'AGC STU-III de l'ID EKMS qui présente la demande doit inscrire son nom en caractères d'imprimerie, signer le formulaire et y incrire la date.

CSE 673 (02-04)

Annexe E – Demande d'établissement de privilèges (PER) pour clés SDNS

Communications Security Establishment | Centre de la sécurité des télécommunications

PROTECTED A (when completed)
PROTÉGÉ A (une fois rempli)

SECURE DATA NETWORK SYSTEM (SDNS) PRIVILEGE ESTABLISHMENT REQUEST (PER)
DEMANDE D'ÉTABLISSEMENT DE PRIVILÈGES (PER) POUR CLÉS SDNS (SECURE DATA NETWORK SYSTEM)

A. ACCOUNT INFORMATION
INFORMATION SUR LE COMPTE

1. FROM/DE — EKMS ID/ID EKMS ☐☐☐☐☐☐
NAME/NOM
NO./Nº — STREET/RUE
CITY/VILLE — PROVINCE — POSTAL CODE/CODE POSTAL

2. TRANSACTION ID/ID DE LA TRANSACTION
☐☐☐☐☐☐ ☐☐☐☐/☐☐/☐☐ ☐☐☐☐
EKMS ID/ID EKMS — DATE (YYYY/MM/DD-AAAA/MM/JJ)

B. USER REPRESENTATIVE – SDNS KEY ORDERING PRIVILEGES
REPRÉSENTANT DE L'UTILISATEUR – PRIVILÈGES DE COMMANDE DE CLÉ SDNS

3. REQUEST TYPE / TYPE DE DEMANDE: ☐ ADD / AJOUT ☐ REPLACE / REMPLACEMENT ☐ DELETE / SUPPRESSION

4. PARTITION CODE TYPE / TYPE DE CODE DE PARTITION: ☐ OPEN / OUVERT ☐ CLOSED / FERMÉ

5. EKMS ACCOUNT NAME / NOM DU COMPTE EKMS
PRIVILEGE FOR EKMS ID / PRIVILÉGE POUR L'ID EKMS

6. PARTITION CODE / CODE DE PARTITION
THE CMAC WILL ASSIGN NEW CLOSED PARTITION CODES.
LE CAGMC ATTRIBUERA DE NOUVEAUX CODES DE PARTITION FERMÉS.

7. AUTHORIZED KEY TYPE / TYPE DE CLÉ AUTORISÉE
☐ CANADIAN TYPE 0 OPERATIONAL / CANADIENNE, OPÉRATIONNELLE DE TYPE 0
☐ CANADIAN TYPE 1 OPERATIONAL / CANADIENNE, OPÉRATIONNELLE DE TYPE 1
☐ CCEB
☐ COALITION
☐ NATO / OTAN

8. MAXIMUM KEY CLASSIFICATION / CLASSIFICATION MAXIMALE DE LA CLÉ
☐ TOP SECRET / TRÈS SECRET
☐ SECRET
☐ CONFIDENTIAL / CONFIDENTIEL
☐ UNCLASSIFIED / NON CLASSIFIÉ
☐ PROTECTED A / PROTÉGÉ A
☐ PROTECTED B / PROTÉGÉ B
☐ PROTECTED C / PROTÉGÉ C

9. KEY PURPOSE / BUT DE LA CLÉ
☐ OPERATIONAL / OPÉRATIONNELLE
☐ TEST
☐ TRAINING CLASSROOM / SALLE DE CLASSE
☐ TRAINING EXERCISE / EXERCICE
☐ DEVELOPMENTAL / DÉVELOPPEMENT
☐ SAMPLE / ÉCHANTILLON
☐ MAINTENANCE

10. EQUIPMENT TYPE / TYPE D'ÉQUIPEMENT
☐ CNES
☐ FASTLANE/KG-75
☐ TACLANE/KG-175
☐ KP/KOK-22A
☐ STE/KOV-14C
☐ SECTERA SWT
☐ OMNI
☐ GSM SWT
☐ OTHER / AUTRE

C. SDNS KMA APPROVAL
APPROBATION DE L'AGC SDNS

I HEREBY CERTIFY THAT THE SDNS USER REPRESENTATIVE AND ALTERNATE USER REPRESENTATIVES REGISTERED WITH THIS EKMS ACCOUNT ARE AUTHORIZED TO ORDER SDNS KEY WITH THE PRIVILEGES INDICATED HEREIN. THE SDNS KMA SIGNING THIS FORM MUST BE REGISTERED WITH THIS EKMS ACCOUNT.
JE, SOUS-SIGNÉ, CERTIFIE QUE LE REPRÉSENTANT DE L'UTILISATEUR ET LES REPRÉSENTANTS SUPPLÉANTS DE L'UTILISATEUR SDNS INSCRITS À CE COMPTE SONT AUTORISÉS À COMMANDER UNE CLÉ SDNS EN VERTU DES PRIVILÈGES INDIQUÉS DANS LA PRÉSENTE. L'AGC QUI SIGNE LE FORMULAIRE DOIT ÊTRE INSCRIT À CE COMPTE EKMS.

NAME/NOM — SIGNATURE — DATE

D. SUBMIT FORMS/ENVOI DES FORMULAIRES

SEND COMPLETED FORMS TO:
COMMUNICATIONS SECURITY ESTABLISHMENT
P.O. BOX 9703, TERMINAL
OTTAWA ON K1G 3Z4
ATTN: CRYPTOMATERIAL MANAGEMENT AND ASSISTANCE CENTRE (CMAC)

VEUILLEZ ENVOYER LE FORMULAIRE AU :
CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS
C.P. 9703, TERMINUS POSTAL
OTTAWA (ONTARIO) K1G 3Z4
ATTENTION : CENTRE D'ASSISTANCE ET DE GESTION DU MATÉRIEL CRYPTOGRAPHIQUE (CAGMC)

IF YOU REQUIRE ASSISTANCE OR HAVE ANY QUESTIONS, PLEASE CONTACT CRYPTOMATERIAL MANAGEMENT AND ASSISTANCE CENTRE (CMAC) AT TEL (613) 991-8600, FAX (613) 991-7440 OR E-MAIL AT CMAC@CSE-CST.GC.CA

SI VOUS AVEZ BESOIN D'AIDE OU SI VOUS AVEZ DES QUESTIONS, VEUILLEZ COMMUNIQUER AVEC LE CENTRE D'ASSISTANCE ET DE GESTION DU MATÉRIEL CRYPTOGRAPHIQUE (CAGMC) PAR TÉLÉPHONE AU (613) 991-8600, PAR FAX AU (613) 991-7440 OU PAR COURRIEL À L'ADRESSE CMAC@CSE-CST.GC.CA.

RESET

CSE 598 (02-04)

INSTRUCTIONS

Section A

Block 1. Enter the name of the EKMS ID submitting the PER.

Block 2. Enter the Transaction ID for the PER. It includes the EKMS ID of the SDNS Key Management Authority (KMA) that is submitting the PER, the current date in YYYYMMDD format, and a one up sequence number for the current calendar year.

Block 3. - Select "Add" to add one SDNS privilege.
- Select "Replace" or "Delete" to delete all SDNS privileges that have the specified EKMS ID and Partition Code combination.

Block 4. - Select "Open" to request ordering privileges for the existing CMAC assigned open partition.
- Select "Closed" to request a new closed partition.

Block 5. Enter the EKMS ID and name of the EKMS ID receiving the privilege.

Block 6. No action required.

Block 7. - Select "Canadian Type 0" if PER Equipment Type is KP/KOK-22A.
- Select "Canadian Type 1" if PER Equipment Type is CNES, FASTLANE/KG-75, TACLANE/KG-175, STE/KOV-14C, Sectera SWT, OMNI or GSM SWT.
Contact the CMAC if CCEB, Coalition or NATO key types are required.

Section B

Block 8. Select one classification. Must not be higher than the privileged EKMS ID's Highest Classification Indicator (HDI) or clearance.

Block 9. **Operational** - if the privileged EKMS ID requires key intended for use on the air for protection of operational information or for the production or secure electrical transmission of key streams. The key classification will include the caveat CRYPTO.
Test if the privileged EKMS ID requires key intended for on the air testing of COMSEC equipment or systems. The key classification will include the caveat CRYPTO.
Training a) classroom - if key required is intended for on the air or off the air classroom training. If the key is for on the air training classification will include the caveat CRYPTO.
b) Exercise - if key required is intended to safeguard transmissions associated with exercises. If used on the air classification will include CRYPTO.
Maintenance - if the privileged EKMS ID requires key intended only for off the air, in-shop use. The key classification will not include the caveat CRYPTO.
Developmental - if the privileged EKMS ID requires key intended for the 'in-process' production of COMSEC material or equipment. The key classification will include the caveat CRYPTO.
Sample - if the privileged EKMS ID requires key intended for off the air demonstration use only. The key classification may include the caveat CRYPTO.

Block 10. Select one Equipment Type key is to be used in.

Section C.

The SDNS KMA of the EKMS ID submitting the PER must print and sign his or her name and enter the current date on the form.

DIRECTIVES

Section A

Case 1. Entrez le nom du compte EKMS qui fait la demande.

Case 2. Entrez l'ID de la transaction de la demande, notamment l'ID EKMS de l'autorité de gestion des clés (AGC) SDNS qui présente la demande, la date en format AAAAMMJJ et un numéro ascendant selon l'année civile en cours.

Case 3. - Choisissez « Ajout » pour ajouter un privilège SDNS.
- Choisissez « Remplacement » ou « Suppression » pour supprimer tous les privilèges SDNS qui portent l'ID EKMS et le code de partition précisés.

Case 4. - Choisissez « Ouvert » afin de demander des privilèges de commande pour la partition ouverte existante attribuée par le CAGMC.
- Choisissez « Fermé » pour demander une nouvelle partition fermée.

Case 5. Entrez l'ID EKMS et le nom de l'ID EKMS qui reçoit le privilège.

Case 6. Aucune mesure requise.

Case 7. - Choisissez « Canadienne, opérationnelle de type 0 » si l'équipement PER est de type KP/KOK-22A.
- Choisissez « Canadienne de type 1 » si l'équipement PER est de type CNES, FASTLANE/KG-75, TACLANE/KG-175, STE/KOV-14C, Sectera SWT, OMNI ou GSM SWT.
Communiquez avec le CAGMC si l'équipement de type CCEB, Coalition ou OTAN est requis.

Section B

Case 8. Choisissez une classification. Ne doit pas être supérieure à l'indicateur de classification le plus élevé (HCI) ou à l'habilitation de l'ID EKMS autorisé.

Case 9. **Opérationnelle** – Si l'ID EKMS autorisé requiert une clé destinée à protéger en direct des renseignements opérationnels ou pour produire et sécuriser une transmission électrique de flots de clés. La classification de la clé comprendra la mention CRYPTO.
Test – Si l'ID EKMS autorisé requiert une clé destinée à la mise à l'essai en ligne de systèmes ou de l'équipement COMSEC. La classification de la clé comprendra la mention CRYPTO.
Formation a) Salle de classe – Si la clé est destinée à la formation en salle de classe en direct ou hors émission. Si la clé est destinée à la formation en direct, la classification de la clé comprendra la mention CRYPTO.
b) Exercices de formation – Si la clé est destinée à la protection des transmissions associées aux exercices en direct, la classification de la clé comprendra la mention CRYPTO.
Maintenance – Si l'ID EKMS autorisé requiert une clé destinée à une utilisation interne hors émission. La classification de la clé ne comprendra pas la mention CRYPTO.
Développement – Si l'ID EKMS autorisé requiert une clé destinée à la protection du matériel ou de l'équipement COMSEC « en cours » de production. La classification de la clé comprendra la mention CRYPTO.
Échantillon – Si l'ID EKMS autorisé requiert une clé destinée à des démonstrations hors émission. La classification de la clé peut comprendre la mention CRYPTO.

Case 10. Choisissez le type d'équipement dans lequel la clé sera utilisée.

Section C.

L'AGC SDNS de l'ID EKMS qui présente la demande doit inscrire son nom en caractères d'imprimerie, signer le formulaire et y inscrire la date.

CSE 598 (02-04)

Annexe F – Demande d'établissement de privilèges (PER) pour clés de signature de message (MSK)

Communications Security Establishment | Centre de la sécurité des télécommunications

PROTECTED A (when completed)
PROTÉGÉ A (une fois rempli)

MESSAGE SIGNATURE KEY (MSK) PRIVILEGE ESTABLISHMENT REQUEST (PER)
DEMANDE D'ÉTABLISSEMENT DE PRIVILÈGES (PER) POUR CLÉS DE SIGNATURE DE MESSAGE (MSK)

A. ACCOUNT INFORMATION/INFORMATION SUR LE COMPTE

1. FROM/DE — EKMS ID/ID EKMS ☐☐☐☐☐☐
NAME/NOM
NO./Nº — STREET/RUE
CITY/VILLE — PROVINCE / CODE POSTAL — POSTAL CODE

2. TRANSACTION ID/ID DE LA TRANSACTION
☐☐☐☐☐☐ ☐☐☐☐/☐☐/☐☐ ☐☐☐☐
EKMS ID/ID EKMS — DATE (YYYY/MM/DD-AAAA/MM/JJ)

B. USER REPRESENTATIVE - MSK KEY ORDERING PRIVILEGES
REPRÉSENTANT DE L'UTILISATEUR - PRIVILÈGES DE COMMANDE DE CLÉ MSK

3. REQUEST TYPE / TYPE DE DEMANDE — ☐ Add / Ajout ☐ Delete / Suppression

4. PRIVILEGE FOR EKMS ID / PRIVILÉGE POUR L' ID EKMS

5. PRIVILEGED EKMS ACCOUNT NAME / NOM DU COMPTE EKMS AUTORISÉ

6. DAO CODE/CODE DAO: 02

7. MAXIMUM KEY CLASSIFICATION / CLASSIFICATION MAXIMALE DE LA CLÉ: SECRET

8. AUTHORIZED KEY TYPE / TYPE DE CLÉ AUTORISÉE
☐ Canadian Type 1/Canadienne de type 1
☐ U.S. Type 1/Américaine de type 1

9. KEY PURPOSE / BUT DE LA CLÉ
☐ Operational/Opérationnelle
☐ Test

10. EQUIPMENT TYPE / TYPE D'ÉQUIPEMENT: KP/KOK-22A

11. EKMS USE INDICATOR / INDICATEUR D'UTILISATION EKMS: Yes/Oui

C. MSK KMA APPROVAL/APPROBATION DE L'AGC MSK

I HEREBY CERTIFY THAT THE MSK USER REPRESENTATIVE AND ALTERNATE USER REPRESENTATIVES REGISTERED WITH THIS EKMS ACCOUNT ARE AUTHORIZED TO ORDER MSK KEY WITH THE PRIVILEGES INDICATED HEREIN. THE MSK KMA SIGNING THIS FORM MUST BE REGISTERED WITH THIS EKMS ACCOUNT.

JE, SOUS-SIGNÉ, CERTIFIE QUE LE REPRÉSENTANT DE L'UTILISATEUR ET LES REPRÉSENTANTS SUPPLÉANTS DE L'UTILISATEUR MSK INSCRITS À CE COMPTE SONT AUTORISÉS À COMMANDER UNE CLÉ MSK EN VERTU DES PRIVILÈGES INDIQUÉS DANS LA PRÉSENTE. L'AGC MSK QUI SIGNE LE FORMULAIRE DOIT ÊTRE INSCRIT À CE COMPTE EKMS.

NAME / NOM — SIGNATURE — DATE

D. SUBMIT FORMS/ENVOI DES FORMULAIRES

SEND COMPLETED FORMS TO:
COMMUNICATIONS SECURITY ESTABLISHMENT
P.O. BOX 9703, TERMINAL
OTTAWA ON K1G 3Z4
ATTN: CRYPTOMATERIAL MANAGEMENT AND ASSISTANCE CENTRE (CMAC)

VEUILLEZ ENVOYER LE FORMULAIRE AU :
CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS
C.P. 9703, TERMINUS POSTAL
OTTAWA (ONTARIO) K1G 3Z4
ATTENTION : CENTRE D'ASSISTANCE ET DE GESTION DU MATÉRIEL CRYPTOGRAPHIQUE (CAGMC)

IF YOU REQUIRE ASSISTANCE OR HAVE ANY QUESTIONS, PLEASE CONTACT CRYPTOMATERIAL MANAGEMENT AND ASSISTANCE CENTRE (CMAC) AT TEL (613) 991-8600, FAX (613) 991-7440 OR E-MAIL AT CMAC@CSE-CST.GC.CA

SI VOUS AVEZ BESOIN D'AIDE OU SI VOUS AVEZ DES QUESTIONS, VEUILLEZ COMMUNIQUER AVEC LE CENTRE D'ASSISTANCE ET DE GESTION DU MATÉRIEL CRYPTOGRAPHIQUE (CAGMC) PAR TÉLÉPHONE AU (613) 991-8600, PAR FAX AU (613) 991-7440 OU PAR COURRIEL À L'ADRESSE CMAC@CSE-CST.GC.CA.

RESET

CSE 673 (02-04)

INSTRUCTIONS FOR THE CANADIAN MESSAGE SIGNATURE KEY PRIVILEGE ESTABLISHMENT REQUEST (PER) FORM

Section A

Block 1. Enter the name of the EKMS ID submitting the PER.

Block 2. Enter the Transaction ID for the PER. It includes the EKMS ID of the MSK Key Management Authority (KMA) that is submitting the PER, the current date in YYYYMMDD format, and a one up sequence number for the current calendar year.

Section B

Block 3. - Select "Add" to add one MSK privilege.
- Select "Delete" to delete all MSK privileges that have the specified EKMS ID and DAO combination.

Block 4. Enter the EKMS ID receiving the privilege.

Block 5. Enter the complete name of the EKMS ID receiving the privilege.

Block 6. No action required.

Block 7. No action required.

Block 8. - Select "Canadian Type 1" for Canadian MSK Type 1 ordering privileges.
- Select "U.S. Type 1" for U.S. MSK Type 1 ordering privileges.

Block 9. - Select "Operational" if key is to be used in a live environment.
- Select "Test" if key is to be used in a test environment.

Block 10. No action required.

Block 11. No action required.

Section C.

The MSK KMA of the EKMS ID submitting the PER must print and sign his or her name and enter the current date on the form.

DIRECTIVES POUR LE FORMULAIRE DE DEMANDE D'ÉTABLISSEMENT DE PRIVILÈGES POUR CLÉS CANADIENNES DE SIGNATURE DE MESSAGE

Section A

Case 1. Entrez le nom du compte EKMS qui fait la demande.

Case 2. Entrez l'ID de la transaction de la demande, notamment l'ID EKMS de l'autorité de gestion des clés (AGC) MSK qui présente la demande, la date en format AAAAMMJJ et un numéro ascendant selon l'année civile en cours.

Section B

Case 3. - Choisissez « Ajout » pour ajouter un privilège MSK.
- Choisissez « Suppression » pour supprimer tous les privilèges qui portent l'ID EKMS et le code DAO précisés.

Case 4. Entrez l'ID EKMS qui reçoit le privilège.

Case 5. Entrez le nom complet de l'ID EKMS qui reçoit le privilège.

Case 6. Aucune mesure requise.

Case 7. Aucune mesure requise.

Case 8. - Choisissez « Canadienne de type 1 » pour des privilèges de commande de clé canadienne MSK de type 1.
- Choisissez « Américaine de type 1 » pour des privilèges de commande de clé américaine MSK de type 1.

Case 9. - Choisissez « Opérationnelle » si la clé servira dans des conditions de travail réelles.
- Choisissez « Test » si la clé servira à des tests.

Case 10. Aucune mesure requise.

Case 11. Aucune mesure requise.

Section C

L'AGC de l'ID EKMS qui présente la demande doit inscrire son nom en caractères d'imprimerie, signer le formulaire et y inscrire la date.

CSE 673 (02-04)

Annexe G – Demande d'établissement de privilèges (PER) pour clés traditionnelles

Communications Security Establishment | Centre de la sécurité des télécommunications

PROTECTED A (when completed)
PROTÉGÉ A (une fois rempli)

TRADITIONAL PRIVILEGE ESTABLISHMENT REQUEST (PER)
DEMANDE D'ÉTABLISSEMENT DE PRIVILÈGES (PER) POUR CLÉS TRADITIONNELLES

A. ACCOUNT INFORMATION/INFORMATION SUR LE COMPTE

1. FROM/DE — EKMS ID/ID EKMS ☐☐☐☐☐☐

NAME/NOM

NO./Nº STREET/RUE

CITY/VILLE PROVINCE POSTAL CODE / CODE POSTAL

2. TRANSACTION ID/ID DE LA TRANSACTION

☐☐☐☐☐☐ ☐☐☐☐/☐☐/☐☐ ☐☐☐☐

EKMS ID/ID EKMS DATE (YYYY/MM/DD-AAAA/MM/JJ)

B. OPM PRIVILEGE/PRIVILÈGE OPM

3. REQUEST TYPE / TYPE DE DEMANDE ☐ INITIAL / INITIALE ☐ CANCEL / ANNULATION

4. PRIVILEGED EKMS ACCOUNT NAME / NOM DU COMPTE EKMS AUTORISÉ

5. PRIVILEGE FOR EKMS ID / PRIVILÈGE POUR L'ID EKMS

C. DSO/DCA APPROVAL/APPROBATION DE L'ASM/ACM

I HEREBY CERTIFY THAT THE ABOVE EKMS ACCOUNT IS GRANTED THE ORDERING PRIVILEGE MANAGER (OPM) PRIVILEGE.
JE, SOUS-SIGNÉ, CERTIFIE QUE LE PRIVILÈGE DE GESTIONNAIRE DES PRIVILÈGES DE COMMANDE (OPM) EST ACCORDÉ AU COMPTE EKMS CI-DESSUS.

NAME/NOM SIGNATURE DATE

D. STAR PRIVILEGE/PRIVILÈGE STAR

6. REQUEST TYPE / TYPE DE DEMANDE ☐ INITIAL / INITIALE ☐ CANCEL / ANNULATION

7. PRIVILEGED EKMS ACCOUNT NAME / NOM DU COMPTE EKMS AUTORISÉ

8. PRIVILEGED FOR EKMS ID / PRIVILÈGE POUR L'ID EKMS

E. OPM APPROVAL/APPROBATION DE L'OPM

I HEREBY CERTIFY THAT THE ABOVE EKMS ACCOUNT IS GRANTED THE SHORT TITLE ASSIGNMENT REQUESTER (START) PRIVILEGE. THE OPM SIGNING THIS FORM MUST BE REGISTERED WITH THIS EKMS ACCOUNT.
JE, SOUS-SIGNÉ, CERTIFIE QUE LE PRIVILÈGE DE DEMANDEUR D'ATTRIBUTION DE TITRE ABRÉGÉ (STAR) EST ACCORDÉ AU COMPTE EKMS CI-DESSUS. L'OPM QUI SIGNE LE FORMULAIRE DOIT ÊTRE INSCRIT À CE COMPTE EKMS.

NAME/NOM SIGNATURE DATE

F. SUBMIT FORMS/ENVOI DES FORMULAIRES

SEND COMPLETED FORMS TO:
COMMUNICATIONS SECURITY ESTABLISHMENT
P.O. BOX 9703, TERMINAL
OTTAWA ON K1G 3Z4
ATTN: CRYPTOMATERIAL MANAGEMENT AND ASSISTANCE CENTRE (CMAC)

VEUILLEZ ENVOYER LE FORMULAIRE AU :
CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS
C.P. 9703, TERMINUS POSTAL
OTTAWA (ONTARIO) K1G 3Z4
ATTENTION : CENTRE D'ASSISTANCE ET DE GESTION DU MATÉRIEL CRYPTOGRAPHIQUE (CAGMC)

IF YOU REQUIRE ASSISTANCE OR HAVE ANY QUESTIONS, PLEASE CONTACT CRYPTOMATERIAL MANAGEMENT AND ASSISTANCE CENTRE (CMAC) AT TEL (613) 991-8600, FAX (613) 991-7440 OR E-MAIL AT CMAC@CSE-CST.GC.CA

SI VOUS AVEZ BESOIN D'AIDE OU SI VOUS AVEZ DES QUESTIONS, VEUILLEZ COMMUNIQUER AVEC LE CENTRE D'ASSISTANCE ET DE GESTION DU MATÉRIEL CRYPTOGRAPHIQUE (CAGMC) PAR TÉLÉPHONE AU (613) 991-8600, PAR FAX AU (613) 991-7440 OU PAR COURRIEL À L'ADRESSE CMAC@CSE-CST.GC.CA.

RESET

CSE 707 (03-04)

INSTRUCTIONS FOR THE TRADITIONAL KEY PRIVILEGE ESTABLISHMENT REQUEST (PER) FORM

Section A

Block 1. Enter the name of the EKMS ID submitting the PER.

Block 2. Enter the Transaction ID for the PER. It includes the EKMS ID submitting the PER, the curent date in YYYYMMDD format, and a one up sequence number for the current calendar year.

Section B

Block 3. - Select "Initial" to add OPM privileges.
- Select "Cancel" to delete OPM privileges.

Block 4. Enter the complete name of the EKMS ID receiving the privilege.

Block 5. Enter the EKMS ID receiving the privilege.

Section C

The DSO/DCA of the EKMS ID submitting the PER must print and sign his or hers name and enter the current date on the form.

Section D

Block 6. - Select "Initial" to add STAR privileges.
- Select "Cancel" to delete STAR privileges.

Block 7. Enter the complete name of the EKMS ID receiving the privilege.

Block 8. Enter the EKMS ID receiving the privilege.

Section E

The OPM of the EKMS ID submitting the PER must print and sign his or hers name and enter the current date on the form.

DIRECTIVES POUR LE FORMULAIRE DE DEMANDE D'ÉTABLISSEMENT DE PRIVILÈGES POUR CLÉS TRADITIONNELLES

Section A

Case 1. Entrez le nom du compte EKMS qui fait la demande.

Case 2. Entrez l'ID de la transaction de la demande, notamment l'ID EKMS qui présente la demande, la date en format AAAAMMJJ et un numéro ascendant selon l'année civile en cours.

Section B

Case 3. - Choisissez « Initiale » pour ajouter des privilèges OPM.
- Choisissez « Annulation » pour supprimer les privilèges OPM.

Case 4. Entrez le nom complet de l'ID EKMS qui reçoit le privilège.

Case 5. Entrez l'ID EKMS qui reçoit le privilège.

Section C

L'ASM/ACM de l'ID EKMS qui présente la demande doit inscrire son nom en caractères d'imprimerie, signer le formulaire et y inscrire la date.

Section D

Case 6. - Choisissez « Initiale » pour ajouter des privilèges STAR.
- Choisissez « Annulation » pour supprimer les privilèges STAR.

Case 7. Entrez le nom complet de l'ID EKMS qui reçoit le privilège.

Case 8. Entrez l'ID EKMS qui reçoit le privilège.

Section E

L'OPM de l'ID EKMS qui présente la demande doit inscrire son nom en caractères d'imprimerie, signer le formulaire et y inscrire la date.

CSE 707 (03-04)

Annexe H – Demande d'établissement de privilèges - avis de confirmation/rejet (PER CRN)

PER CRN
Protected A

Printed : Mar 02, 2005 02:18 PM
Page 1 of 1

EKMS MESSAGE :

Message ID :	845550-20050302-54239	Message Date :	Mar 02, 2005
Source EKMS ID :	845550	Source Element Name :	
Destination EKMS ID :	841234	Destination Element Name :	
Subject :			

Transaction Type	Transaction ID	Transaction Information Label
SDNS PER CRN	845550-20050302-55240	FOUO

PER CRN TRANSACTION :

Transaction ID :	845550-20050302-55240	Transaction Date :	Mar 02, 2005
Source EKMS ID :	845550	Source Element Name :	
Destination EKMS ID :	841234	Destination Element Name :	
CCF KPF Transaction Status :	Approved	Transmission Method :	Electronic
Overall Status :	Confirmation	Per Type :	SDNS
		PER Transaction ID :	841234-20050209-2
Privilege For EKMS ID :	841234	Element Name :	841234
Comments :			

NOTHING FOLLOWS

Page intentionnellement laissée en blanc

Annexe I – Avis de demande de privilèges (OPN)

SNDS OPN (Privilege Recipient) **Protected A**

Printed : Mar 02, 2005 02:18 PM

Page 1 of 1

EKMS MESSAGE :

Message ID :	845550-20050302-54240	Message Date :	Mar 02, 2005
Source EKMS ID :	845550	Source Element Name :	
Destination EKMS ID :	841234	Destination Element Name :	
Subject :			

Transaction Type	Transaction ID	Transaction Information Label
Order Privilege Notice	845550-20050302-55241	FOUO

PER CRN TRANSACTION:

Transaction ID :	845550-20050302-55241	Transaction Date :	Mar 02, 2005
Source EKMS ID :	845550	Source Element Name :	
Destination EKMS ID :	841234	Destination Element Name :	
CCF KPF Transaction Status :	Approved	Transmission Method :	Paper
Overall Status :	Sent		
Privileged At EKMS ID :	845550	Element Name :	
Privileging EKMS ID :	841234	Element Name :	
Privilege For EKMS ID :	841234	Element Name :	
Privilege Est. Request Type :	Add	Equipment (Device) Type :	KG 175
Maximum Classification :	Unclassified	Key Type Level :	Type 1
Key Purpose (OP/Test Indicator) :	Testing	EKMS Use (Allowed) Ind. :	N

Partition Code	Seed/Op Ind.	EKR Priv. Ind.	ALC
3001	Operational	N	

NOTHING FOLLOWS

Page intentionnellement laissée en blanc

Annexe J – Demande de clé STU III

Communications Security Establishment / Centre de la sécurité des télécommunications

PROTECTED A (when completed)
PROTÉGÉ A (une fois rempli)

STU-III KEY ORDER REQUEST
DEMANDE DE CLÉ STU-III

1. FROM/DE — EKMS ID/ID EKMS ☐☐☐☐☐☐

NAME/NOM

NO./N° STREET/RUE

CITY/VILLE PROVINCE POSTAL CODE/CODE POSTAL

2. TRANSACTION ID/ID DE LA TRANSACTION

☐☐☐☐☐☐ ☐☐☐☐/☐☐/☐☐ ☐☐☐☐

EKMS ID/ID EKMS DATE (YYYY/MM/DD-AAAA/MM/JJ)

3. TYPE OF KEY/TYPE DE CLÉ

☐ TYPE 1 OPERATIONAL/OPÉRATIONNELLE DE TYPE 1
☐ TYPE 1 SEED/ENCLENCHEMENT DE TYPE 1
☐ TYPE 2 OPERATIONAL/OPÉRATIONNELLE DE TYPE 2
☐ CANADIAN/CANADIENNE
☐ U.S./AMÉRICAINE

4. EQUIPMENT TYPE /TYPE D'ÉQUIPEMENT

☐ STU-III
☐ KOV-14C SERIAL NO/ N° DE SÉRIE KOV-14C
☐ CIPHERTAC SERIAL NO./N° DE SÉRIE CIPHERTAC

5. EKMS STU-III KEY ORDER/COMMANDE DE CLÉ STU-III EKMS

☐ YES/OUI ☐ NO/NON

6. ITEM # # ART.	7. QTY QTÉ	8. CLASSIFICATION	9. CODE	10. DAO CODE CODE DAO	11. EKMS ID ID EKMS	12. ADDITIONAL IDENTIFICATION DATA DONNÉES D'IDENTIFICATION ADDITIONNELLES	13. REMARKS OBSERVATIONS
		☐ P ☐ C ☐ S ☐ TS					
		☐ P ☐ C ☐ S ☐ TS					
		☐ P ☐ C ☐ S ☐ TS					
		☐ P ☐ C ☐ S ☐ TS					
		☐ P ☐ C ☐ S ☐ TS					
		☐ P ☐ C ☐ S ☐ TS					
		☐ P ☐ C ☐ S ☐ TS					
		☐ P ☐ C ☐ S ☐ TS					
		☐ P ☐ C ☐ S ☐ TS					
		☐ P ☐ C ☐ S ☐ TS					

14. SHIP TO/À — EKMS ID/ID EKMS ☐☐☐☐☐☐

NAME/NOM

NO./N° STREET/RUE

CITY/VILLE PROVINCE POSTAL CODE/CODE POSTAL

15. I HAVE VERIFIED THAT THE INTENDED USERS OF THE ABOVE KEYING MATERIAL POSSESS A SECURITY CLEARANCE CONSISTENT WITH THE CLASSIFICATION OF THE REQUESTED KEY.

J'AI VÉRIFIÉ QUE LES UTILISATEURS PRÉVUS DU MATÉRIEL DE CHIFFREMENT CI-DESSUS DÉTIENNENT L'HABILITATION DE SÉCURITÉ CORRESPONDANTE À LA CLASSIFICATION DE LA CLÉ DEMANDÉE.

SIGNATURE OF USER REPRESENTATIVE / SIGNATURE DU REPRÉSENTANT DES UTILISATEURS

PRINT NAME / NOM EN CARACTÈRES D'IMPRIMERIE

16. SPECIAL INSTRUCTIONS/DIRECTIVES SPÉCIALES

SEND COMPLETED FORMS TO:
COMMUNICATIONS SECURITY ESTABLISHMENT
P.O. BOX 9703, TERMINAL
OTTAWA ON K1G 3Z4
ATTN: CRYPTOMATERIAL MANAGEMENT AND ASSISTANCE CENTRE (CMAC)

VEUILLEZ ENVOYER LE FORMULAIRE AU :
CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS
C.P. 9703, TERMINUS POSTAL
OTTAWA (ONTARIO) K1G 3Z4
ATTENTION : CENTRE D'ASSISTANCE ET DE GESTION DU MATÉRIEL CRYPTOGRAPHIQUE (CAGMC)

IF YOU REQUIRE ASSISTANCE OR HAVE ANY QUESTIONS, PLEASE CONTACT CRYPTOMATERIAL MANAGEMENT AND ASSISTANCE CENTRE (CMAC) AT TEL (613)991-8600, FAX (613) 991-7440 OR E-MAIL AT CMAC@CSE-CST.GC.CA

SI VOUS AVEZ BESOIN D'AIDE OU SI VOUS AVEZ DES QUESTIONS, VEUILLEZ COMMUNIQUER AVEC LE CENTRE D'ASSISTANCE ET DE GESTION DU MATÉRIEL CRYPTOGRAPHIQUE (CAGMC) PAR TÉLÉPHONE AU (613) 991-8600, PAR FAX AU (613) 991-7440 OU PAR COURRIEL À L'ADRESSE CMAC@CSE-CST.GC.CA.

RESET

CSE 696 (02-04)

INSTRUCTIONS

Block 1. Enter the name, address and EKMS ID of the account submitting the order.

Block 2. Enter the Transaction ID for the order. It includes the EKMS ID that is submitting the order, the current date in YYYYMMDD format, and a one up number for the current month, starting back at 1 each month (eg. 0001, 0002, etc).

Block 3. Select the key type and the country of origin.
- Select "Canadian" if Canadian key is required.
- Select "U.S." if American key is required.

Block 4. Select the equipment type to be loaded with the STU-III key. If selected CipherTAC or KOV-14C indicate their serial number in the remarks column.

Block 5. Select yes if the key is to be use for the LMD/KP.

Block 6. Enter line item number starting at 1.

Block 7. Indicate the number of keys required for this line item number.

Block 8. Select the classification of the key being ordered. (P=PROTECTED, C=CONFIDENTIAL, S=SECRET, TS=TOP SECRET)

Block 9. Optional. Enter the appropriate Class 6 code for the key being ordered.

01 PROTECTED C
02 PROTECTED B
03 PROTECTED A
10 SCI
20 U.S.
25 MOBILE

Block 10. Enter the appropriate DAO code for the key.

Block 11. If selected "yes" at Block 5, enter the EKMS ID of the key being ordered.

Block 12. Enter any additional identification information for the key up to a maximum of 16 characters per line, to a maximum of 2 lines. Do not repeat the DAO description. Note that the maximum characters available, including those used for the DAO description, cannot exceed 50 characters and therefore the number of character available for use in the additional identification information may be limited.

Block 13. Enter any remarks that apply to this line item.

Block 14. The key will be shipped to this EKMS ID. All key on a single order form must be shipped to a single EKMS ID.

Block 15. The ordering EKMS ID's STU-III User Representative must sign the form.

Block 16. Enter any special instructions that apply to the key order.

DIRECTIVES

Case 1. Entrez le nom, l'adresse et l'ID EKMS du compte qui fait la demande.

Case 2. Entrez l'ID de transaction de la commande, notamment l'ID EKMS de la personne qui présente la commande, la date en format AAAAMMJJ et un numéro ascendant selon le mois en cours, qui recommence à 1 chaque mois (par ex. 0001, 0002, etc).

Case 3. Sélectionnez le type de clé et le pays d'origine.
- Choisissez « Canadienne » si une clé canadienne est exigée.
- Choisissez « Américaine » si une clé américaine est exigée.

Case 4. Sélectionnez le type d'équipement à charger au moyen de la clé STU-III. S'il s'agit d'un dispositif CipherTAC ou KOV-14C, indiquez leur numéro de série dans la case observations.

Case 5. Si la clé doit être utilisée pour le LMD/KP, cochez la case Oui.

Case 6. Entrez le numéro de ligne d'article en commençant par 1.

Case 7. Indiquez le nombre de clés demandées pour ce numéro de ligne d'article.

Case 8. Choisissez la classification de la clé commandée. (P = PROTÉGÉ, C = CONFIDENTIEL, S = SECRET, TS = TRÈS SECRET)

Case 9. Facultative. Entrez le code de classe 6 de la clé commandée.

01 PROTÉGÉ C
02 PROTÉGÉ B
03 PROTÉGÉ A
10 SCI
20 U.S.
25 MOBILE

Case 10. Entrez le code DAO pour la clé.

Case 11. Si vous avez répondu Oui à la case 5, entrez l'ID EKMS de la clé commandée.

Case 12. Entrez les données d'identification additionnelles relatives à la clé (pas plus de 16 caractères par ligne et sur un maximum de deux lignes). Ne répétez pas la description DAO. Notez que le nombre maximal de caractères, y compris ceux utilisée dans la description DAO, ne peut excéder 50. Le nombre de caractères pouvant être inscrits pour les données additionnelles risque donc d'être limité.

Case 13. Entrez toute observation qui s'applique à la ligne d'article en question.

Case 14. La clé sera expédiée à cet ID EKMS. Toute clé indiquée dans une seule commande doit être expédiée au même ID EKMS.

Case 15. Le représentant des utilisateurs STU-III de l'ID EKMS qui passe la commande doit signer la demande.

Case 16. Entrez toute autre directive qui s'applique à cette commande de clé.

CSE 696 (02-04)

Annexe K – Demande de clés - SDNS

Communications Security Establishment / Centre de la sécurité des télécommunications

PROTECTED A (when completed)
PROTÉGÉ A (une fois rempli)

SECURE DATA NETWORK SYSTEM (SDNS) KEY ORDER REQUEST
DEMANDE DE CLÉS – SECURE DATA NETWORK SYSTEM (SDNS)

1. FROM/DE — EKMS ID/ID EKMS ☐☐☐☐☐☐

NAME/NOM

NO./N° STREET/RUE

CITY/VILLE PROVINCE POSTAL CODE/CODE POSTAL

2. TRANSACTION ID/ID DE LA TRANSACTION

☐☐☐☐☐☐ ☐☐☐☐/☐☐/☐☐ ☐☐☐☐

EKMS ID/ID EKMS DATE (YYYY/MM/DD-AAAA/MM/JJ)

3. PARTITION CODE TYPE/TYPE DE CODE DE PARTITION

☐ OPEN/OUVERT
☐ CLOSED/FERMÉ
☐☐☐☐☐☐☐☐☐☐ TEN DIGIT CODE/CODE À 10 CHIFFRES

4. EQUIPMENT TYPE/TYPE D'ÉQUIPEMENT

☐ CNES ☐ KP/KOK-22A ☐ GSM SWT
☐ FASTLANE/KG-75 ☐ STE/KOV-14C
☐ TACLANE/KG-175 ☐ OMNI
☐ SECTERA SWT ☐ OTHER/AUTRE

5. KEY TYPE/TYPE DE CLÉ

☐ TYPE 0 OPERATIONAL/TYPE 0 OPÉRATIONNELLE
☐ TYPE 1 OPERATIONAL/TYPE 1 OPÉRATIONNELLE

6. KEY PURPOSE/OBJET DE LA CLÉ

☐ OPERATIONAL/OPÉRATIONNELLE ☐ MAINTENANCE ☐ TRAINING CLASSROOM/SALLE DE CLASSE ☐ SAMPLE/ÉCHANTILLON
☐ DEVELOPMENTAL/DÉVELOPPEMENT ☐ TEST ☐ TRAINING EXERCISE/EXERCICE

7. COUNTRY OF ORIGIN / PAYS D'ORIGINE

☐ CANADA ☐ COALITION
☐ U.S./É.-U. ☐ NATO/OTAN
☐ CCEB
☐ OTHER/AUTRE

8. HANDLING RESTRICTIONS / RESTRICTIONS DE TRAITEMENT

☐ NO RESTRICTIONS/AUCUNE
☐ BENIGN FILL ONLY / REMPLISSAGE BÉNIN
☐ TPI

9. ACCESS CONTROL SCHEDULE / CONTRÔLE D'ACCÈS

☐ NONE/AUCUN
☐ COMMS
☐ DISTRIBUTION

10. DEVICE CAPABILITIES / CAPACITÉS DU DISPOSITIF

☐ LMD/KP OR CRYPTO UNIT / LMD/KP OU UNITÉ CRYPTO
☐ AUTH. ASCII ID/ID ASCII AUTORISÉ
☐ TEST

11. ITEM NO / N° ART.	12. QTY / QTÉ	13. CLASSIFICATION	14. EKMS ID / ID EKMS	15. DESCRIPTOR ASCII ID / ID ASCII DESCRIPTEUR	16. DELIVERY METHOD / MÉTHODE DE LIVRAISON	17. REMARKS / OBSERVATIONS
		☐ U/NC ☐ C ☐ S ☐ TS			☐ BET ☐ DTD ☐ KSD ☐ KOV-14C	
		☐ U/NC ☐ C ☐ S ☐ TS			☐ BET ☐ DTD ☐ KSD ☐ KOV-14C	
		☐ U/NC ☐ C ☐ S ☐ TS			☐ BET ☐ DTD ☐ KSD ☐ KOV-14C	
		☐ U/NC ☐ C ☐ S ☐ TS			☐ BET ☐ DTD ☐ KSD ☐ KOV-14C	

18. DTD LOADING INSTRUCTIONS/DIRECTIVES DE CHARGEMENT DU DTD

ITEM NO / N° ART.	DTD TEXT ID / ID TEXTE DU DTD	EKMS ID / ID EKMS	DTD SER# / N° SÉRIE DTD	CIK# / N° CIK	FIRST EDN / 1ÈRE ÉD.	LAST EDN / DERN. ÉD.	EDN QTY / Nbre D'ÉD.	QTY/EDN / Nbre/ÉD.	TOTAL COPIES / Nbre TOT. COPIES	SEG/EDN / SEG./ÉD.	TOT SEG / Nbre TOT. SEG.

19. SHIP TO/À — EKMS ID/ID EKMS ☐☐☐☐☐☐

NAME/NOM

NO./N° STREET/RUE

CITY/VILLE PROVINCE POSTAL CODE/CODE POSTAL

20. I HAVE VERIFIED THAT THE INTENDED USERS OF THE ABOVE KEYING MATERIAL POSSESS A SECURITY CLEARANCE CONSISTENT WITH THE CLASSIFICATION OF THE REQUESTED KEY.

J'AI VÉRIFIÉ QUE LES UTILISATEURS PRÉVUS DU MATÉRIEL DE CHIFFREMENT CI-DESSUS DÉTIENNENT L'HABILITATION DE SÉCURITÉ CORRESPONDANT À LA CLASSIFICATION DE LA CLÉ DEMANDÉE.

SIGNATURE OF USER REPRESENTATIVE / SIGNATURE DU REPRÉSENTANT DES UTILISATEURS

PRINT NAME / NOM EN CARACTÈRES D'IMPRIMERIE

SEND COMPLETED FORMS TO:
COMMUNICATIONS SECURITY ESTABLISHMENT
P.O. BOX 9703, TERMINAL
OTTAWA ON K1G 3Z4
ATTN: CRYPTOMATERIAL MANAGEMENT AND ASSISTANCE CENTRE (CMAC)

VEUILLEZ ENVOYER LE FORMULAIRE AU :
CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS
C.P. 9703, TERMINUS POSTAL
OTTAWA (ONTARIO) K1G 3Z4
ATTENTION : CENTRE D'ASSISTANCE ET DE GESTION DU MATÉRIEL CRYPTOGRAPHIQUE (CAGMC)

IF YOU REQUIRE ASSISTANCE OR HAVE ANY QUESTIONS, PLEASE CONTACT CRYPTOMATERIAL MANAGEMENT AND ASSISTANCE CENTRE (CMAC) AT TEL (613) 991-8600, FAX (613)991-7440 OR E-MAIL AT CMAC@CSE-CST.GC.CA

SI VOUS AVEZ BESOIN D'AIDE OU SI VOUS AVEZ DES QUESTIONS, VEUILLEZ COMMUNIQUER AVEC LE CENTRE D'ASSISTANCE ET DE GESTION DU MATÉRIEL CRYPTOGRAPHIQUE (CAGMC) PAR TÉLÉPHONE AU (613) 991-8600, PAR FAX AU (613) 991-7440 OU PAR COURRIEL À L'ADRESSE CMAC@CSE-CST.GC.CA.

CSE 697 (11-03)

INSTRUCTIONS

Block 1. Enter the name, address and the EKMS ID of the account submitting the order.

Block 2. Enter the Transaction ID for the order. It includes the EKMS ID of the SDNS User Representative that is submitting the order, the current date in YYYYMMDD format, and a one up sequence number for the current month, starting back at 1 each month (eg. 0001, 0002, etc).

Block 3. Select "Open" unless it is for a specific network. In that case select "Closed" and specify the ten digit code assigned by CMAC.

Block 4. Select one Equipment Type.

Block 5. - Select Key "Type 0" if Equipment Type is KP/KOK-22A.
- Select Key "Type 1" if Equipment Type is CNES, Fastlane/KG-75, Taclane/KG-175, STE/KOV-14C, SECTERA SWT, OMNI or GSM SWT.

Block 6. Select one of the options described below:

Operational If the privileged EKMS ID requires key intended for use on the air for protection of operational information or for the production or secure electrical transmission of key streams. The key classification will include the caveat CRYPTO.

Test If the privileged EKMS ID requires key intended for on the air testing of COMSEC equipment or systems. The key classification will include the caveat CRYPTO.

Training a) Classroom - if key required is intended for on the air or off the air classroom training. If the key is for on the air training the key classification will include the caveat CRYPTO.
b) Exercise - if key required is intended to safeguard transmissions associated with exercises. If used on the air classification will include CRYPTO.

Maintenance If the privileged EKMS ID requires key intended only for off the air, in-shop use. The key classification will not include the caveat CRYPTO.

Sample If the privileged EKMS ID requires key intended for off the air demonstration use only. The key classification may include the caveat CRYPTO.

Block 7. - Select "Canadian" if Canadian key is required.
- Select "U.S." if American key is required.
Contact the CMAC if CCEB, Coalition or NATO key types are required

Block 8. - Select "No Restrictions" if key classification is UNCLASSIFIED, CONFIDENTIAL or SECRET.
- Select "TPI" if key classification is TOP SECRET.

Block 9. Optional field.
- Select "None" if this feature is not required.
- Select "Comms" if Key Type is Type 1 Operational.
- Select "Distribution" if Key Type is Type 0 Operational. (for keys ordered for the LMD/KP)

Block 10. - Select "LMD/KP" or "CU" if Equipment Type is KP/KOK-22A.
- Select "Auth. ASCII ID" if Equipment Type is STE/KOV-14C.
- Select "Test" if Key Purpose is Test.

Block 11. Enter line iatem number starting at 1.

Block 12. Enter the number of keys required.

Block 13. Select one classification if Equipment Type is CNES, Fastlane/KG-75, Taclane/KG-175, STE/KOV-14C, SECTERA SWT, OMNI or GSM SWT.
Select :
UNCLASSIFIED - if Key Purpose is Test, Training, Sample or Maintenance.
SECRET - if end user EKMS ID Highest Classification Indicator or clearance is SECRET, Key Purpose is Operational and if Equipment Type is KP/KOK-22A.
SECRET and TOP SECRET - if end user EKMS ID Highest Classification Indicator or clearance is TOP SECRET, Key Purpose is Operational and if Equipment Type is KP/KOK-22A.

Block 14. Enter end user EKMS ID if Equipment Type is KP/KOK-22A.

Block 15. Mandatory field if Equipment Type is CNES, STE/KOV-14C, SECTERA SWT, OMNI or GSM SWT. Except for the CNES the format is "{DAO CODE}\{DAO Descriptor}".

Block 16. Select one Delivery Method. It is recommended that fully automated EKMS ID's select BET to receive keys electronically. Note that only certain types of key may be delivered electronically from the CCF.

Block 17. Provide the serial number of the ECU if Equipment Type DTD or STE/KOV-14C is selected. Enter any other remarks for that line item number.

Block 18. Mandatory field when using a DTD.
Item No - Enter the line item number.
DTD Text ID - Optional. Enter a common text identifier that will be associated with each key loaded into the DTD. Only one text identifier allowed for each DTD.
EKMS ID - Enter the EKMS ID where the DTD and keys will be shipped.
DTD Ser# - Enter the serial number of the DTD that will be loaded with key from this order.
CIK# - CMAC will process this request on a case-by-case basis only. If approved by the CMAC, enter the CIK slot numbers in which the key will be loaded. Valid numbers are 1 to 8. Client must ship CIK's with DTD to the CSE NDA. The CIK's must be clearly labeled and identify its associated DTD.
First Edn - Enter the first, or only, edition of key from this order to be loaded into this DTD.
Last Sdn - Enter the last, or only, edition of key from this order to be loaded into this DTD.
Edn Qty - Enter the total number of editions of key from this order that is to be loaded into this DTD.
Qty/Edn - Enter the number of copies of key per edition that is to be loaded into this DTD. A DTD can be loaded with 22 Type 1 Firefly keys (11 during changeover year).
Total Copies -Enter the total number of copies that is to be loaded into this DTD. A DTD can be loaded with 22 Type 1 Firefly keys (11 during changeover year).
Seg/ Edn - Enter "1".
Tot Seg Qty - Enter the number of segments to be loaded into this DTD. "Total Qty" multiplied by "Seg Per Edn".

Block 19. The key will be shipped to this EKMS ID. All key on a single order form must be shipped to a single EKMS ID.

Block 20. The ordering EKMS ID's SDNS User Representative must sign the form.

DIRECTIVES

Case 1. Entrez le nom, l'adresse et l'ID EKMS du compte qui fait la demande.

Case 2. Entrez l'ID de transaction de la commande, notamment l'ID EKMS du représentant des utilisateurs SDNS qui passe la commande, la date en format AAAAMMJJ et un numéro ascendant selon le mois en cours, qui recommence à 1 chaque mois (par ex. 0001, 0002, etc).

Case 3. Choisissez « Ouvert », à moins qu'il ne s'agisse d'un réseau en particulier. S'il s'agit d'un réseau en particulier, choisissez « Fermé » et inscrivez le code à dix chiffres attribué par le CAGMC.

Case 4. Choisissez un type d'équipement.

Case 5. - Choisissez le type de clé 0 si l'équipement est de type KP/KOK-22A.
- Choisissez le type de clé 1 si l'équipement est de type CNES, Fastlane/KG-75, Taclane/KG-175, STE/KOV-14C, SECTERA SWT, OMNI ou GSM SWT.

Case 6. Choisissez l'une des options suivantes :

Opérationnelle Si l'ID EKMS autorisé requiert une clé destinée à protéger en ligne des renseignements opérationnels ou pour produire et sécuriser une transmission électrique de séquences de clés. La classification de la clé comprendra la mention CRYPTO.

Test Si l'ID EKMS autorisé requiert une clé destinée à la mise à l'essai en ligne de systèmes ou de l'équipement COMSEC. La classification de la clé comprendra la mention CRYPTO.

Formation a) Salle de classe – Si la clé est destinée à la formation en salle de classe en ligne ou hors émission. Si la clé est destinée à la formation en ligne, la classification de la clé comprendra la mention CRYPTO.
b) Exercices de formation – Si la clé est destinée à la protection des transmissions associées aux exercices. Si la clé est destinée aux exercices en ligne, la classification de la clé comprendra la mention CRYPTO.

Maintenance Si l'ID EKMS autorisé requiert une clé destinée à une utilisation interne hors émission. La classification de la clé ne comprendra pas la mention CRYPTO.

Échantillon Si l'ID EKMS autorisé requiert une clé destinée à des démonstrations hors émission. La classification de la clé peut comprendre la mention CRYPTO.

Case 7. - Choisissez « Canada » si une clé canadienne est exigée.
- Choisissez « É.-U. » si une clé américaine est exigée.
Communiquez avec le CAGMC si une clé de type CCEB, Coalition ou OTAN est exigée.

Case 8. - Choisissez « Aucune » si la clé porte l'une des classifications suivantes : NON CLASSIFIÉ, CONFIDENTIEL ou SECRET.
- Choisissez « TPI » si la clé est classifiée TRÈS SECRET.

Case 9. Champ facultatif.
- Choisissez « Aucun » si la fonction n'est pas nécessaire.
- Choisissez « COMMS » si la clé est de type 1 opérationnelle.
- Choisissez « Distribution » si la clé est de type 0 opérationnelle (LMD/KP).

Case 10. - Choisissez « LMD/KP » ou « Unité crypto. » s'il s'agit d'équipement de type KP/KOK-22A.
- Choisissez « ID ASCII autorisé » s'il s'agit d'équipement de type STE/KOV-14C.
- Choisissez « Test » si la clé servira à des tests.

Case 11. Entrez le numéro de ligne d'article en commençant par 1.

Case 12. Entrez le nombre de clés requises.

Case 13. Choisissez une classification s'il s'agit d'équipement de type CNES, Fastlane/KG-75, Taclane/KG-175 ,STE/KOV-14C, SECTERA SWT, OMNI ou GSM SWT.
Choisissez :
NON CLASSIFIÉ – Si l'objet de la clé est l'un des suivants : test, formation, échantillon ou maintenance.
SECRET – Si l'indicateur du niveau de classification le plus élevé (HCI) ou l'habilitation de sécurité de l'ID EKMS de l'utilisateur correspond à SECRET, et qu'il s'agit d'une clé opérationnelle et d'équipement de type KP/KOK-22A.
SECRET et TRÈS SECRET – Si l'indicateur du niveau de classification le plus élevé (HCI) ou l'habilitation de sécurité de l'ID EKMS de l'utilisateur correspond à TRÈS SECRET, et qu'il s'agit d'une clé opérationnelle et d'équipement de type KP/KOK-22A.

Case 14. Entrez l'ID EKMS de l'utilisateur s'il s'agit d'équipement de type KP/KOK-22A.

Case 15. Champ obligatoire s'il s'agit d'un CNES, STE/KOV-14C, SECTERA SWT, OMNI ou GSM SWT. Le format à l'exception du CNES est le suivant : « {DAO CODE}\{DAO Descriptor} ».

Case 16. Choisissez une méthode de livraison. Il est recommandé que les ID EKMS entièrement automatisés choisissent BET afin de recevoir les clés par voie électronique. À noter que seuls certains types de clé peuvent être livrés par voie électronique de l'ICC.

Case 17. Inscrivez le numéro de série de l'ECU s'il s'agit d'équipement de type DTD ou STE/KOV-14C. Entrez toute observation qui s'applique à la ligne d'article en question.

Case 18. Champ obligatoire si vous utilisez un DTD.
No d'art. – Entrez le numéro de ligne d'article.
ID texte du DTD – Facultatif. Entrez un identificateur texte commun qui sera associé à chaque clé chargée dans le DTD. Un seul identificateur texte est permis par DTD.
ID EKMS – Entrez l'ID EKMS où seront expédiés le DTD et les clés.
No série DTD – Entrez le numéro de série du DTD dans lequel seront chargées les clés de cette commande.
No CIK – Le CAGMC traitera cette demande au cas par cas uniquement. Si celui-ci donne son approbation, entrez les numéros de compartiments de la CIK où la clé doit être chargée. Les numéros valides sont les suivants : 1 à 8. Le client doit expédier les CIK avec le DTD à l'AND du CST. Les CIK doivent être clairement étiquetées et porter le nom du DTD auquel elles sont associées.
1ère éd. – Entrez la première, ou la seule, édition de clé de cette commande à charger dans le DTD.
Dern. éd. – Entrez la dernière, ou la seule, édition de clé de cette commande à charger dans le DTD.
Nbre d'éd. – Entrez le nombre total d'éditions de clé de cette commande à charger dans le DTD.
Nbre/éd. – Entrez le nombre de copies de clé par édition à charger dans le DTD. Un DTD peut recevoir 22 clés Firefly de type 1 (11 lors d'une année de transition).
Nbre tot. copies – Entrez le nombre total de copies à charger dans le DTD. Un DTD peut recevoir 22 clés Firefly de type 1 (11 lors d'une année de transition).
Seg./éd. – Entrez «1».
Nbre tot. seg. – Entrez le nombre de segments à charger dans le DTD (Nbre total seg. multiplié par Seg./éd).

Case 19. La clé sera expédiée à cet ID EKMS. Toute clé indiquée dans une seule commande doit être expédiée au même ID EKMS.

Case 20. Le représentant des utilisateurs SDNS de l'ID EKMS qui passe la commande doit signer le formulaire.

Annexe L – Demande de clés de signature de message (MSK)

Communications Security Establishment | Centre de la sécurité des télécommunications

PROTECTED A (when completed)
PROTÉGÉ A (une fois rempli)

MESSAGE SIGNATURE KEY (MSK) KEY ORDER REQUEST
DEMANDE DE CLÉS DE SIGNATURE DE MESSAGE (MSK)

1. FROM/DE — EKMS ID/ID EKMS ☐☐☐☐☐☐ NAME/NOM NO./N° STREET/RUE CITY/VILLE PROVINCE POSTAL CODE/CODE POSTAL	2. TRANSACTION ID/ID DE LA TRANSACTION ☐☐☐☐☐☐ ☐☐☐☐/☐☐/☐☐ ☐☐☐☐ EKMS ID/ID EKMS DATE (YYYY/MM/DD-AAAA/MM/JJ)
3. DAO CODE/CODE DAO 02	4. EQUIPMENT TYPE/TYPE D'ÉQUIPEMENT KP/KOK-22A
5. KEY TYPE/TYPE DE CLÉ ☐ Canadian Type 1/Canadienne de type 1 ☐ U.S. Type 1/Américaine de type 1	6. KEY PURPOSE/BUT DE LA CLÉ ☐ Operational/Opérationnelle ☐ Test
7. EKMS USE INDICATOR/INDICATEUR D'UTILISATION EKMS Yes/Oui	

8. ITEM # / # ART.	9. QTY / QTÉ	10. CLASSIFICATION / CLASSIFICATION	11. FREE FORM ID / ID ADDITIONNELS	12. REMARKS / REMARQUES
		SECRET	☐☐☐☐☐☐:	
		SECRET	☐☐☐☐☐☐:	
		SECRET	☐☐☐☐☐☐:	
		SECRET	☐☐☐☐☐☐:	
		SECRET	☐☐☐☐☐☐:	
		SECRET	☐☐☐☐☐☐:	

13. SHIP TO/À — EKMS ID/ID EKMS ☐☐☐☐☐☐ NAME/NOM NO./N° STREET/RUE CITY/VILLE PROVINCE POSTAL CODE/CODE POSTAL	14. I HAVE VERIFIED THAT THE INTENDED USERS OF THE ABOVE KEYING MATERIAL POSSESS A SECURITY CLEARANCE CONSISTENT WITH THE CLASSIFICATION OF THE REQUESTED KEY. J'AI VÉRIFIÉ QUE LES UTILISATEURS PRÉVUS DU MATÉRIEL DE CHIFFREMENT CI-DESSUS DÉTIENNENT L'HABILITATION DE SÉCURITÉ CORRESPONDANT À LA CLASSIFICATION DE LA CLÉ DEMANDÉE. SIGNATURE OF USER REPRESENTATIVE / SIGNATURE DU REPRÉSENTANT DES UTILISATEURS — PRINT NAME / NOM EN CARACTÈRES D'IMPRIMERIE

SEND COMPLETED FORMS TO: COMMUNICATIONS SECURITY ESTABLISHMENT P.O. BOX 9703, TERMINAL OTTAWA ON K1G 3Z4 ATTN: CRYPTOMATERIAL MANAGEMENT AND ASSISTANCE CENTRE (CMAC)	**VEUILLEZ ENVOYER LE FORMULAIRE AU :** CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS C.P. 9703, TERMINUS POSTAL OTTAWA (ONTARIO) K1G 3Z4 ATTENTION : CENTRE D'ASSISTANCE ET DE GESTION DU MATÉRIEL CRYPTOGRAPHIQUE (CAGMC)
IF YOU REQUIRE ASSISTANCE OR HAVE ANY QUESTIONS, PLEASE CONTACT CRYPTOMATERIAL MANAGEMENT AND ASSISTANCE CENTRE (CMAC) AT TEL (613) 991-8600, FAX (613) 991-7440 OR E-MAIL AT CMAC@CSE-CST.GC.CA	SI VOUS AVEZ BESOIN D'AIDE OU SI VOUS AVEZ DES QUESTIONS, VEUILLEZ COMMUNIQUER AVEC LE CENTRE D'ASSISTANCE ET DE GESTION DU MATÉRIEL CRYPTOGRAPHIQUE (CAGMC) PAR TÉLÉPHONE AU (613) 991-8600, PAR FAX AU (613) 991-7440 OU PAR COURRIEL À L'ADRESSE CMAC@CSE-CST.GC.CA.

RESET

CSE 665 (02-04)

INSTRUCTIONS

Block 1. Enter the name, address, and the EKMS ID of the account submitting the order.

Block 2. Enter the Transaction ID for the order. It includes the EKMS ID of the MSK User Representative that is submitting the order, the current date in YYYYMMDD format, and the one up sequence number for the current calendar year.

Block 3. No action required.

Block 4. No action required.

Block 5. - Select "Canadian Type 1" for Canadian MSK Type 1 key.
- Select "U.S. Type 1" for U.S. MSK Type 1 key.

Block 6. - Select "Operational" if key is to be used in a live environment.
- Select "Test" if key is to be used in a test environment.

Block 7. No action required.

Block 8. Enter order item number.

Block 9. Enter the number of keys required.

Block 10. No action required.

Block 11. Enter the end user's six digit EKMS ID and their Privilege Certificate Manager's (PCM's) six digit EKMS ID. Enter 845999 as the PCM EKMS ID if key purpose is operational. Enter 845550 as the PCM EKMS ID if key purpose is test. A colon separates the two EKMS ID's (:).

Block 12. Enter any remarks for that line item number.

Block 13. Enter the full mailing address and EKMS ID of the account that the key will be shipped to.

Block 14. The ordering EKMS ID's MSK User Representative must sign the form.

DIRECTIVES

Case 1. Entrez le nom, l'adresse et l'ID EKMS du compte qui passe la commande.

Case 2. Entrez l'ID de la transaction de la commande, notamment l'ID EKMS du représentant de l'utilisateur MSK qui présente la demande, la date en format AAAAMMJJ et un numéro ascendant selon l'année civile en cours.

Case 3. Aucune mesure requise.

Case 4. Aucune mesure requise.

Case 5. - Choisissez « Canadienne de type 1 » pour une clé canadienne MSK de type 1.
- Choisissez « Américaine de type 1 » » pour une clé américaine MSK de type 1.

Case 6. - Choisissez « Opérationnelle » si la clé servira dans des conditions de travail réelles.
- Choisissez « Test » si la clé servira à des tests.

Case 7. Aucune mesure requise.

Case 8. Entrez le numéro de la ligne d'article.

Case 9. Entrez la quantité de clés requises.

Case 10. Aucune mesure requise.

Case 11. Entrez l'ID EKMS de six chiffres de l'utilisateur final et l'ID EKMS de six chiffres du gestionnaire de certificats des privilèges (PCM). Entrez 845999 comme ID EKMS du PCM si le but de la clé est « opérationnelle ». Entrez 845999 comme ID EKMS du PCM si le but de la clé est « test ». Deux points (:) séparent les ID EKMS.

Case 12. Entrez toute remarque se rapportant à cette ligne d'article.

Case 13. Entrez l'adresse postale complète et l'ID EKMS du compte où la clé sera expédiée.

Case 14. Le représentant de l'utilisateur MSK de l'ID EKMS qui passe la commande doit signer le formulaire.

CSE 665 (02-04)

Annexe M – Demande de clés traditionnelles

Communications Security Establishment | Centre de la sécurité des télécommunications

PROTECTED A (when completed)
PROTÉGÉ A (une fois rempli)

TRADITIONAL KEY ORDER REQUEST
DEMANDE DE CLÉS TRADITIONNELLES

1. EKMS ID / ID EKMS ☐☐☐☐☐☐

EKMS ACCOUNT NAME
NOM DU COMPTE EKMS _____

2. DATE (YYYY/MM/DD-AAAA/MM/JJ) ☐☐☐☐/☐☐/☐☐

3. ITEM # / # ART.	4. SHORT TITLE / TITRE ABRÉGÉ	5. EQUIPMENT TYPE / TYPE D'ÉQUIPEMENT	6. COPIES/QTY / COPIES PAR ÉDITION	7. Nº OF EDN / Nbre D'ÉDITIONS	8. EDITION LETTERS / LETTRES D'ÉDITION	9. TARGET DATE (YY-MM-DD) / DATE LIMITE (AA-MM-JJ)	10. CLASS / CLASS	11. FORMAT / FORMAT	12. APPROVAL / RÉFÉRENCE LIÉE	13. REMARKS REFERENCE / REMARQUES À L'APPROBATION

14. I HAVE VERIFIED THAT THE INTENDED USERS OF THE ABOVE KEYING MATERIAL POSSESS A SECURITY CLEARANCE CONSISTENT WITH THE CLASSIFICATION OF THE REQUESTED KEY.
J'AI VÉRIFIÉ QUE LES UTILISATEURS PRÉVUS DU MATÉRIEL DE CHIFFREMENT CI-DESSUS DÉTIENNENT L'HABILITATION DE SÉCURITÉ CORRESPONDANTE À LA CLASSIFICATION DE LA CLÉ DEMANDÉE.

SIGNATURE OF USER REPRESENTATIVE / SIGNATURE DU REPRÉSENTANT DES UTILISATEURS _____

PRINT NAME / NOM EN CARACTÈRES D'IMPRIMERIE _____

SEND COMPLETED FORMS TO:
COMMUNICATIONS SECURITY ESTABLISHMENT
P.O. BOX 9703, TERMINAL
OTTAWA ON K1G 3Z4
ATTN: CRYPTOMATERIAL MANAGEMENT AND ASSISTANCE CENTRE (CMAC)

VEUILLEZ ENVOYER LE FORMULAIRE AU :
CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS
C.P. 9703, TERMINUS POSTAL
OTTAWA (ONTARIO) K1G 3Z4
ATTENTION : CENTRE D'ASSISTANCE ET DE GESTION DU MATÉRIEL CRYPTOGRAPHIQUE (CAGMC)

IF YOU REQUIRE ASSISTANCE OR HAVE ANY QUESTIONS, PLEASE CONTACT CRYPTOMATERIAL MANAGEMENT AND ASSISTANCE CENTRE (CMAC) AT TEL (613) 991-8600, FAX (613) 991-7440 OR E-MAIL AT CMAC@CSE-CST.GC.CA

SI VOUS AVEZ BESOIN D'AIDE OU SI VOUS AVEZ DES QUESTIONS, VEUILLEZ COMMUNIQUER AVEC LE CENTRE D'ASSISTANCE ET DE GESTION DU MATÉRIEL CRYPTOGRAPHIQUE (CAGMC) PAR TÉLÉPHONE AU (613) 991-8600, PAR FAX AU (613) 991-7440 OU PAR COURRIEL À L'ADRESSE CMAC@CSE-CST.GC.CA.

RESET

CSE 673 (03-04)

INSTRUCTIONS

Block 1. Enter the EKMS ID and name of the account ordering the key.

Block 2. Enter the date that the order is submitted.

Block 3. Enter a one up number identifying the line item.

Block 4. Enter the Short title of the key being ordered. "CSE/537/1" would be a typical keytape short title. "CAKAE 2 845550" would be a typical KG-175 short title example. If a continuing requirement, obtain short title from your last order.

Block 5. Enter the equipment type the key is being ordered for. "KG-175" or "KG-84 Keytape" would be typical entries. Also specify 'Operational', 'Maintenance', 'Test', 'Classroom Training', 'Exercise Training".

Block 6. Enter the number of copies per edition required.

Block 7. Enter the number of editions being ordered. If you require a 12-month supply, enter 12. We do not recommend ordering quantities in excess of one year.

Block 8. Enter the edition letters progress from AA to ZZ, "AA-AL" would be the correct entry for 12 editions when the short title is ordered for the first time.

Block 9. Enter date that you would like to receive the material.

Block 10. Select one classification of TOP SECRET, SECRET, CONFIDENTIAL, UNCLASSIFIED, or PROTECTED A, B or C followed by the caveat "CRYPTO" if required.

Block 11. This column is for keytape only. A typical entry would be AA, a two-letter code-meaning canister contains 31 variables, 1 copy of each, and each segment has a daily cryptoperiod.

Block 12. For CMAC use.

Block 13. Enter any remarks for that line item number. If the order is for KG-175 Pre-Placed key, enter the serial number of the DTD to be shipped to the CCF and loaded with key.

Block 14. The ordering EKMS ID's OPM or STAR must sign the form.

DIRECTIVES

Case 1. Entrez l'ID EKMS et le nom du compte qui commande la clé.

Case 2. Entrez la date à laquelle la commande est transmise.

Case 3. Entrez un numéro ascendant correspondant à la ligne d'article.

Case 4. Entrez le titre abrégé de la clé commandée. Par exemple, « CSE/537/1» est un titre abrégé typique de bande-clé et « CAKAE 2 845550 » est un titre abrégé typique du dispositif KG-175. S'il s'agit d'un article qui a déjà été commandé, veuillez prendre le titre abrégé dans votre commande précédente.

Case 5. Entrez le type d'équipement pour lequel la clé est commandée. Par exemple, « KG-175 » et « Bande-clé KG-84 » seraient des entrées possibles. Veuillez également préciser le but de la clé en ajoutant « opérationnelle », « maintenance », « test », « salle de classe » ou « exercice ».

Case 6. Entrez le nombre de copies requis par édition.

Case 7. Entrez le nombre d'éditions commandées. Si vous avez besoin d'un approvisionnement de 12 mois, entrez 12. Nous vous recommandons de ne pas commander d'articles pour plus d'un an.

Case 8. Entrez la tranche des lettres d'édition de AA à ZZ; « AA-AL » serait une entrée appropriée pour 12 éditions lorsqu'un titre abrégé est commandé pour la première fois.

Case 9. Entrez la date à laquelle vous aimeriez recevoir le matériel.

Case 10. Choisissez une classification parmi TRÈS SECRET, SECRET, CONFIDENTIEL, NON CLASSIFIÉ et PROTÉGÉ A, B ou C, ainsi que la mention CRYPTO s'il y a lieu.

Case 11. Cette colonne se rapporte uniquement à la bande-clé. Un bon exemple d'entrée serait « AA », un code à deux lettres signifiant que le distributeur comprend 31 variables, une copie de chacune, et que chaque segment a une période cryptographique d'une journée.

Case 12. Réservé au CAGMC.

Case 13. Entrez toute remarque se rapportant à ce numéro de ligne d'article. S'il s'agit de la commande d'une clé pré-placée KG-175, entrez le numéro de série du DTD qui sera expédié à l'ICC et dans lequel la clé sera chargée.

Case 14. L'OPM ou le STAR de l'ID EKMS qui passe la commande doit signer le formulaire.

CSE 673 (03-04)